Best Practices Guide

McAfee Endpoint Encryption 7.0 Patch 1 Software

For use with ePolicy Orchestrator 4.6 Software

Contents

Preface **5**

About this guide 5

Audience 5

Conventions 5

Find product documentation 6

1 Introduction **7**

Comprehensive McAfee Endpoint Encryption 7

Purpose of this guide 7

Abbreviations 8

2 Design overview **9**

Support for the self-encrypting (Opal from Trusted Computing Group) drive 9

Endpoint Encryption Policies 10

Configure UBP enforcement 10

PBA in Endpoint Encryption 7.0 Patch 1 11

How Endpoint Encryption works 12

McAfee ePO requirements 12

Requirements testing for client systems 13

3 Software configuration and policies **15**

Active Directory configuration 16

EE LDAP Server User/Group Synchronization 17

Recommended Product Settings Policy 20

Recommended User-Based Policy Settings 28

Checklist for using Intel® AMT and EEPC 30

Phased deployment strategies 31

4 Deployment and activation **33**

Basic preparations and recommendations 34

High level process of the installation 36

Client task to deploy the EEAgent and Endpoint Encryption packages 36

Add group users 39

Users 39

Add local domain users 39

Endpoint Encryption activation sequence 41

Activate Endpoint Encryption using Add local domain users 42

Skip Unused Sectors 43

5 Operations and maintenance **45**

How does disabling/deleting a user in Active Directory affect the Endpoint Encryption user 45

Manage Machine Keys 46

Configure role based access control for managing Endpoint Encryption 48

EEPC 7.0 Patch 1 scalability 49

6 Migration and upgrade 51
Best practices for migration and upgrade 51
Export user assignments from 5.x.x database 53
Import user assignments to McAfee ePO 54
Upgrade to EEPC 7.0 Patch 1 55

7 Use ePolicy Orchestrator to report client status 57
Track the progress of the deployment and encryption status 58
Report encryption status from McAfee ePO 58

Index 61

Preface

This guide provides the information on best practices on using McAfee Endpoint Encryption.

Contents

- *About this guide*
- *Find product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	**Note:** Additional information, like an alternate method of accessing an option.
	**Tip:** Suggestions and recommendations.
	**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.
	**Warning:** Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Introduction

McAfee Endpoint Encryption provides superior encryption across a variety of endpoints such as desktops and laptops. The Endpoint Encryption solution uses strong access control with Pre-Boot Authentication (PBA) and a NIST approved algorithm to encrypt data on endpoints. Encryption and decryption are completely transparent to the end user and performed without hindering system performance.

Administrators can easily implement and enforce security policies that control how sensitive data is encrypted. These policies allow the administrators to monitor real-time events and generate reports to demonstrate compliance with internal and regulatory requirements.

Endpoint Encryption has the advantage over other competitive encryption products, because it engages encryption prior to loading of the Windows or Mac operating system, while data is at rest.

Contents

- *Comprehensive McAfee Endpoint Encryption*
- *Purpose of this guide*

Comprehensive McAfee Endpoint Encryption

This guide indicates Endpoint Encryption (EE) as the term to describe EEPC and EEMac. The content that refers to the term Endpoint Encryption (EE) is applicable to both EEPC and EEMac. Procedures and other details that are different for EEPC and EEMac setup are described in separate sections indicating its individual product name, for example, EEPC or EEMac.

The McAfee Endpoint Encryption (EE) suite provides multiple layers of defense against data loss with several integrated modules that address specific areas of risk. The suite provides protection for individual computers, roaming laptops, MacBooks, and Mac desktops with 64-bit Extensible Firmware Interface (EFI).

This guide discusses these McAfee Endpoint Encryption solutions:

- McAfee Endpoint Encryption for PC
- McAfee Endpoint Encryption for Mac

Purpose of this guide

This guide suggests best practices for deployment and activation. It also discusses optimization and maintenance before and after deployment.

When planning a large scale deployment of EEPC/EEMac 7.0 Patch 1, it is important to understand:

- The features of McAfee® ePolicy Orchestrator® (McAfee ePO™)
- The process of scaling the back end component

- AD/LDAP
- The associated Endpoint Encryption communication

This document encapsulates the professional opinions of Endpoint Encryption certified engineers, and is not an exact science. You must understand both the product and the environment in which it will be used, before deciding on an implementation strategy. Calculations and figures in this guide are based on field evidence and not theoretical system testing; they are our **best advice** at the time of writing.

Please review the best practices and use the guidelines that best fit your environment.

Abbreviations

The following table lists the abbreviations used in this document.

Table 1-1 Abbreviations

Titles	Designations
AD	Active Directory
ASCI	Agent Server Communication Interval
BIOS	Basic Input/Output System
DN	Domain Name
EEM	Endpoint Encryption Manager
EEPC	Endpoint Encryption for PC
EEMac	Endpoint Encryption for Mac
ePO	ePolicy Orchestrator
LDAP	Lightweight Directory Access Protocol
MBR	Master Boot Record
NIST	National Institute of Standards and Technology
OS	Operating System
OU	Organizational Unit
PC	Personal Computer
SSO	Single Sign On
UBP	User-Based Policy
GPT	GUID Partition Table
HFS	Mac OS X Extended File System
HFS+	Mac OS X Extended (Journaled) File System

2 Design overview

The McAfee ePO server is a central store of configuration information for all systems, servers, policies, and users.

Each time the administrator initiates a policy update, or an Agent Server Communication Interval (ASCI), the EEPC/EEMac protected system connects with McAfee ePO.

The Endpoint Encryption protected system queries McAfee ePO for any configuration updates and downloads them. An example of updates are a new user assigned (by the administrator) to the client system, a change in policies, or a change in server settings specified by the administrator.

The Endpoint Encryption protected system also updates any changes on the client system back to the McAfee ePO server, for example, change of user's password token data.

Contents

- *Support for the self-encrypting (Opal from Trusted Computing Group) drive*
- *Endpoint Encryption Policies*
- *PBA in Endpoint Encryption 7.0 Patch 1*
- *How Endpoint Encryption works*
- *McAfee ePO requirements*
- *Requirements testing for client systems*

Support for the self-encrypting (Opal from Trusted Computing Group) drive

EEPC 7.0 Patch 1 provides better management facility for the Opal drive, which is a self-contained and standalone Hard Disk Drive (HDD) that conforms to the Trusted Computing Group (TCG) Opal standard.

The Opal drive is always encrypted by the on board crypto processor. However, it may or may not be locked. Though the Opal drive handles all of the encryption, it needs to be managed by a management software like McAfee ePolicy Orchestrator. If the Opal drive is not managed, it behaves and responds like a normal HDD.

The combination of EEPC and McAfee ePO for Opal provides:

- Centralized management
- Reporting and recovery functionality
- A secure Pre-Boot Authentication that unlocks the Opal drive
- An efficient user management
- Continuous policy enforcement

The overall experience and tasks of an administrator and users in installing and using EEPC are exactly the same regardless of whether the target system has an Opal drive or a normal HDD. The installation of the product extension, deployment of the software packages, policy enforcement, and the method of management are all the same for both systems with Opal and HDD.

Endpoint Encryption Policies

Endpoint Encryption is managed through the McAfee ePO server, using a combination of Product Settings, User-Based and Add Local Domain User Settings policies.

The McAfee ePO console allows the administrator to enforce policies across groups of computers, or a single computer. Any new policy enforcement through McAfee ePO overrides the existing policy that is already set on the individual systems. There are three types of policies: Product Settings, User-Based Policies, and Add Local Domain User Settings. Product Settings Policies are specific to a system or a group of systems. User Based Policies are specific to a user, or a group of users, on a system or a group of systems. Add Local Domain User Settings are specific to adding a blacklist of users to the ALDU functionality.

The Product Settings Policy controls the behavior of the EEPC/EEMac installed systems. For example, it contains the options for enabling encryption, enabling automatic booting, and controlling the theme for the Pre-Boot environment.

The User-Based Policy controls the parameters for EEPC/EEMac user accounts. For example, it contains the options for selecting a token type (including password and smartcard) and password content rules.

Using Add Local Domain User Settings Policies, you can use the Add Local Domain User Settings policy and add a blacklist of users to the ALDU functionality. Users added to the blacklist are excluded from the list of users assigned by the ALDU function.

Configure UBP enforcement

By default, all users inherit the default User-Based Policy assigned to a system and are prevented from using Policy Assignment Rules for EEPC UBP in order to provide maximum system scalability. User Based policies should be kept to a minimum when possible since UBPs impact performance and activation time. For EEMac the UBP enforcement feature is same as the Product Setting policy.

Before you begin

You must have appropriate permissions to perform this task.

To allow a user to use a non-default User Based Policy, you must enable UBP enforcement for that user. This allows Policy Assignment Rules to be executed to select a specific non-default UBP for the user. If not enabled, Policy Assignment Rules are not performed and the user inherits the default UBP.

Failing to assign UBP using Policy Assignment Rule to users, with UBP enforcement enabled, might cause EEPC activation to fail.

User Based Policies in Endpoint Encryption 7.0 Patch 1

A requirement of EEPC 7.0 Patch 1 is that you need to specify which groups of users are allowed or not to use the Policy Assignment Rules. The allowed users get their required User Based Policies. Users that are not allowed to use the Policy Assignment Rules inherit the default User Based Policies assigned to the system.

For EEMac the Policy Assignment Rule selection criteria only uses System Properties, which allows you to assign the rule to System(s) in a group. Because of this only a single policy can be assigned to a Mac system at a time. As a result, all users on the Mac client will have the same policy setting.

Task

1 Click **Menu** | **Reporting** | **Queries**. The Queries page opens.

2 Select **Endpoint Encryption** from Shared Groups in Groups pane. The standard EE query list appears.

3 Run the **EE: Users** query to list all the Endpoint Encryption Users.

4 Select a user(s) from the list to enforce the policy.

5 Click **Actions** | **Endpoint Encryption** | **Configure UBP enforcement**. The Configure UBP enforcement page appears with Enable and Disable options.

6 Select **Enable** or **Disable**, then click **OK** to configure the UBP enforcement state. On selecting Enable, Policy Assignment Rules are enabled for the selected users, and a specific UBP is assigned to the user according to the rule defined.

At each ASCI, ePolicy Orchestrator enforces all the relevant user-based policies to each client in addition to the user-based policy for the logged on user configured with UBP enforcement.

PBA in Endpoint Encryption 7.0 Patch 1

On BIOS-based systems, the EEPC operating system provides security by booting prior to Windows and requiring Pre-Boot Authentication before the user is allowed to access the main operating system. On UEFI-based systems, the EEPC software runs as a trusted application providing the same level of functionality.

PBA in **EEMac** is a firmware application that acts as a trusted authentication layer by serving as an extension of the boot firmware and guarantees a secure, tamper-proof environment external to the Mac operating system. Firmware is the combination of persistent memory and program code and data stored in it.

The PBA in Endpoint Encryption prevents Windows or Mac from loading until the user has authenticated with the correct password. It eliminates the possibility that one of the millions of lines of the OS code can compromise the privacy of personal or company data.

The PBA provided by Endpoint Encryption has proven time and time again as the best Data Protection solution in the market. The PBA solution is an unmatched best practice to be followed by any organization for system security and data protection.

How Endpoint Encryption works

A boot sequence is executed by the BIOS (Windows) or firmware (Mac) leading to the starting of the bootable operating systems.

Operating system	Remarks
Windows	The boot sequence is the initial set of operations that the computer performs when it is switched on. A boot loader (or a bootstrap loader) is a short computer program that loads the main operating system for the computer. The BIOS first looks at a boot record, which is the logical area **zero** (or starting point) point of the disk drive, known as Master Boot Record (MBR), which contains the boot loader. **On BIOS systems** EEPC alters the MBR; the BIOS loads the modified MBR that will then load the sector chain containing the Pre-Boot environment. This Pre-Boot screen then prompts the user for authentication credentials, which might be a password, smart card, or token. **On UEFI systems** The UEFI specification defines a boot manager, a firmware policy engine that is in charge of loading the OS loader and all necessary drivers. The boot configuration is controlled by a set of global NVRAM variables, including boot variables that indicate the paths to the loaders. PBA is a UEFI application started by the UEFI Boot Manager before the Windows bootloader uses standard UEFI protocols for GUI implementation (Graphics Output Protocol, Simple Pointer Protocol, etc.) GPT Headers and Partition Tables cannot be encrypted: • The data in these regions is required before the disk is unlocked • The disk would not be recognized as a valid GPT disk and the system would be unable to boot
Mac	The BootROM firmware is the initial set of operations that a Mac computer performs when it is switched on. When BootROM (or the user) selects Mac OS X as the operating system to boot, the control passes to the BootX boot loader. The BootX loads the kernel. The kernel then initializes various Mac/BSD data structures and finally loads the Mac OS X desktop for user. When EEMac becomes active, it alters the NVRAM variables on Mac and loads the Pre-Boot Authentication window for the user. When the user successfully authenticates to PBA, the Mac OS X loads by decrypting the initial sectors of the disk. Finally passing the control, the EEMac host process runs under Mac OS X for further crypt operations.

After the user enters valid authentication credentials, the operating system starts to load and the user can use the computer in a normal way.

Encrypting a PC or Mac with EEPC or EEMac respectively is the best and the most important practice that any organization can have for protecting their data.

McAfee ePO requirements

The McAfee ePO server is a central store of configuration information for all systems, servers, policies, and users. It can be installed only on Windows Server 2003 or 2008 operating systems. For detailed

information about installing or using McAfee ePO, see the ePolicy Orchestrator product documentation for version 4.6.

Supported environments for McAfee ePO and Endpoint Encryption

As new operating systems and service packs are released, the original Product Guides for McAfee ePO and Endpoint Encryption might not reflect the current McAfee support policy for those platforms. To view supported environments for McAfee ePO and Endpoint Encryption, read these Knowledge Base articles:

- EEPC— https://kc.mcafee.com/corporate/index?page=content&id=KB76804
- EEMac—https://kc.mcafee.com/corporate/index?page=content&id=KB68921

For more details, you can also refer to the *McAfee Endpoint Encryption - 7.0 Patch 1 Product Guide*.

Hardware requirements for McAfee ePO

For details on the hardware requirements for McAfee ePO, See the product documentation for your version of McAfee ePO.

Software requirements

For details on the software requirements for McAfee ePO and McAfee Agent, see the Release Notes for EEPC and EEMac.

Clients communicating with McAfee ePO 4.6 through VPN disappear from the McAfee tree. For more information, refer to the KnowledgeBase article https://kc.mcafee.com/corporate/index?page=content&id=KB52949.

Requirements testing for client systems

McAfee Endpoint Encryption for PC requirements must be met before it can be installed on a client system.

McAfee Endpoint Encryption GO (EEGO) 7.0 Patch 1

McAfee provides the McAfee Endpoint Encryption GO (EEGO) 7.0 Patch 1 utility for system administrators to determine which systems are compatible for installing and activating EEPC. EEGO runs a set of compatibility tests on a client system, and then creates a report through the McAfee ePO console that summarizes the readiness of the managed systems.

The McAfee Endpoint Encryption system policy can be configured to prevent activation of encryption on client systems that fail EEGO testing.

Make sure that EEGO is not a pre-requisite for installing EEPC and it comes as a separate package.

If the system is connected to the McAfee ePO server, the system sends the readiness status to McAfee ePO through McAfee Agent.

The overall EEGO installation and deployment process can be simplified into the following steps.

This assumes that the user has already successfully installed McAfee ePO and has McAfee Agent installed on all appropriate client systems that successfully communicates with McAfee ePO.

1. Install the EEGO extension (EEGO.ZIP) in McAfee ePO. Repeat the same procedures used for installing the product extension.
2. Check in the EEGO software package (EegoPackage.ZIP) to McAfee ePO. Repeat the same procedures used for checking in the product package.
3. Deploy Endpoint Encryption GO to the client system. Repeat the same procedures used for the product deployment task.
4. Enforce EEGO policies to the client system.

After restarting, the client system communicates with the McAfee ePO server and pulls down the assigned Endpoint Encryption GO policy, runs the tests and reports the system diagnostic information according to the defined policies.

If you select the **Only activate if health check (Endpoint Encryption : Go) passes** option and then uninstall EEGO from the client, it is not possible to deselect this option. As a result of this, EEPC will fail to activate.

Also, the status of EEGO endpoints can be monitored through various chart representations available in McAfee ePO.

EEGO runs these tests for installing EEPC:

- Incompatible product detection: SafeBoot, HP ProtectTools 2009, Bitlocker, PointSec, Truecrypt, GuardianEdge, Symantec Endpoint Encryption, SafeGuardEasy and PGP Whole Disk Encryption.
- Smart Controller predictive failure, a test that reports if the Operating System is reporting that the S.M.A.R.T. controller is indicating an imminent failure.
- Disk Status, a test for BIOS based systems, reports if the disk (MBR and partition structure) is suitable to install EEPC.

  Make sure to note that EEGO is not supported for UEFI systems.
- Datachannel communication status, a test reporting of the success or failure of the Datachannel communication from the client to the McAfee ePO server.
- Datachannel communication delay, a test in milliseconds of the delay of the communication between the McAfee ePO server and the endpoint.

If any of these requirements is not valid, and the EEPC system policy is configured to abandon activation if the EEGO tests fail, EEPC activation will be abandoned.

EEGO is capable of detecting a series of circumstances that might impact the rollout of EEPC. However, EEGO does not replace the need to perform due diligence testing prior to a rollout.

Pre-boot Smart Check

The Pre-Boot Smart Check is functionality in EEPC that performs various tests to ensure that the EEPC pre-boot environment can work successfully on a device. It will test the areas that have been identified to cause incompatibility issues in the past.

If a device fails the Pre-Boot Smart Check it will not activate EEPC and will not proceed. You can view the audit log to get the latest information on any progress of the check from the last time the device synchronized with McAfee ePO.

The Pre-Boot Smart Check can be used in conjunction with EEGO and help administrators during initial deployments. EEGO will perform checks and validation in the operating system, and the Pre-Boot Smart Check will perform checks/validations outside of the operating system. The combined usage can give administrators the highest confidence of a successful deployment.

3 Software configuration and policies

When planning for a rollout and deployment of EEPC/EEMac, we recommend that you understand the following important tasks correctly.

- How to configure an LDAP server in McAfee ePO
- How to schedule and run the **EE LDAP Server User/Group Synchronization** task
- How to configure policies and different strategies for phased deployments

Contents

- *Active Directory configuration*
- *EE LDAP Server User/Group Synchronization*
- *Recommended Product Settings Policy*
- *Recommended User-Based Policy Settings*
- *Checklist for using Intel® AMT and EEPC*
- *Phased deployment strategies*

Active Directory configuration

Endpoint Encryption users are not created from the McAfee ePO server. They are assigned to the client systems from an Active Directory (AD) registered in ePolicy Orchestrator. The McAfee ePO Server is responsible for the connection between the client and AD.

Check for the correct format of the Domain name, Username, and Server Address while registering the LDAP server in McAfee ePO.

The AD users are different from Endpoint Encryption users.

- A user exists in AD.
- User string is added as a Pre-Boot user.
- User string is then matched to AD to verify if it exists.
- User string is used to login into Pre-Boot.
- If the correct SSO options are selected, then the user string is compared [string comparison **similar** to java **string.matches()**].
- The end user perceives that he is logging only once using a single user, however, the underlying mechanism still uses two different users one to logon at Pre-Boot and another to logon against Active Directory.

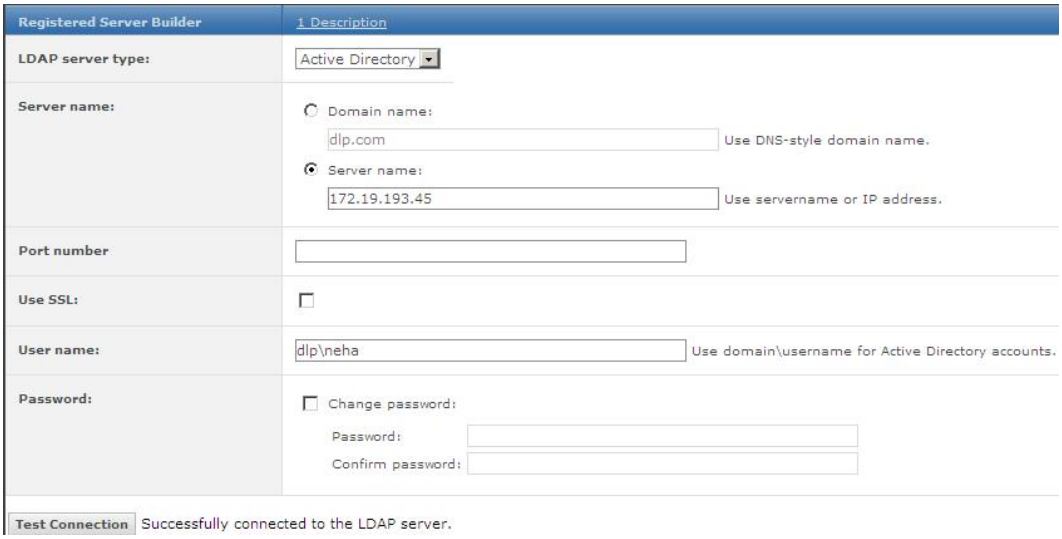


Figure 3-1 Register Active Directory

It is better to key in the IP address of the domain server in the Server name field than entering the domain name of the domain server. This is due to the potential problems caused by DNS failures and/or canonical DNS servers failing to resolve the LDAP server(s) for the domain.

There could be instances when the Test Connection would get through even if you haven't keyed in the domain name and the username in correct format, however, the error could hinder the Endpoint Encryption activation. One of the potential outcomes is that a successful logon to the LDAP server might work because the DNS resolves to LDAP_A but when the task is run the DNS resolves to LDAP_B and the logon fails. Other potential outcomes can be that the logon happens against a LDAP server containing the full copy of the AD structure, a later resolution points to a newly added server that only contains a subset of the AD structure.

EE LDAP Server User/Group Synchronization

Make sure you use the correct user attribute format in the EE LDAP Server User/Group Synchronization task. Match the correct user attributes in the fields.

Figure 3-2 EE LDAP Server User/Group Synchronization

Username

The value of this field determines the form of the PBA username. For example, if the username value is set to samaccountname, the user has to provide the samaccountname at the Pre-Boot Authentication page.

Display Name

The value of this field decides the form of the username displayed in ePolicy Orchestrator (**Menu** | **Reporting** | **Queries** | **Endpoint Encryption** | **EE: Users** and **Menu** | **Data Protection** | **Encryption Users** | **Actions** | **Endpoint Encryption** | **View Users**) pages. For example, if the username attribute is set to samaccountname and Display Name attribute is set to userprincipalname, the username appears as name *(paul)@domain.com*.

If the Display name attribute is set to userprincipalname, the username appears as *name* (paul)*@mcafee.com* whereas the user will be allowed to log on with the name value *name* (paul). (This can be different depending on the attribute selected in the username field and value of the attribute set in the LDAP).

If the attribute value used for Username or Display Name is not set in the LDAP server for any user, Endpoint Encryption uses the attribute distinguished name for that particular object.

Account Control

This attribute checks for the status of the user, for example, if the user is enabled or disabled on the LDAP server.

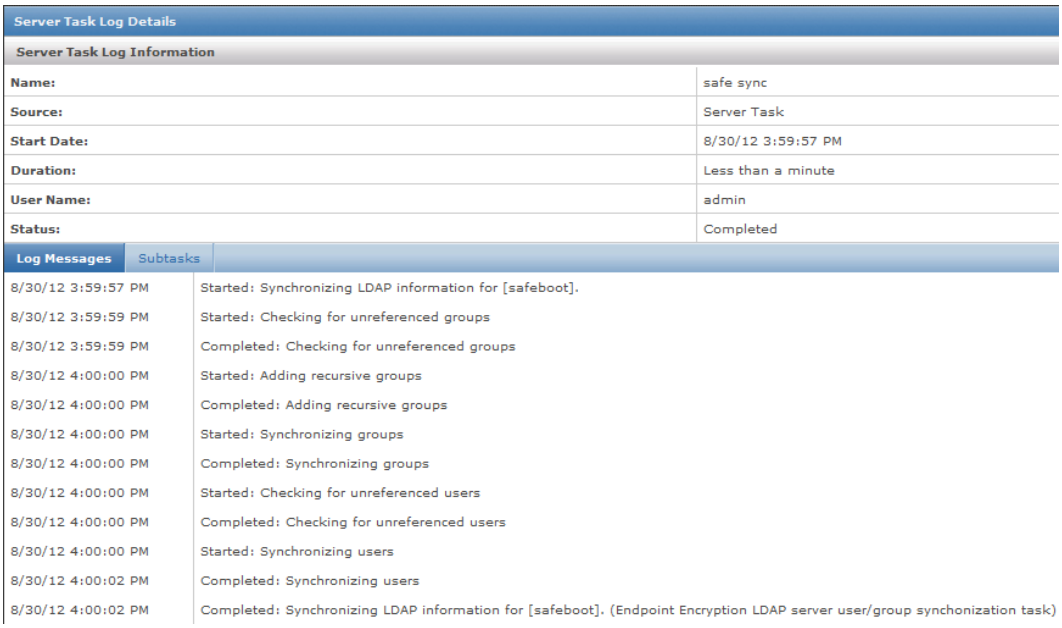
User Certificate

The User Certificate attribute is used by the McAfee ePO Server to determine which certificate should be sent from ePolicy Orchestrator to the client, for example, smartcard tokens. It is better to clear this attribute when you use the Password only token. Setting this attribute can accumulate large amount of certificate data in the ePO database and impact LDAP performance; therefore, you can remove the certificate query from EE LDAP Server User/Group Synchronization while using the Password only token.

After changing the attribute value for any of the fields, the EE LDAP Server User/Group Synchronization task needs to be run, to make sure the ePolicy Orchestrator database is updated with the new values.

EE LDAP Server User/Group Synchronization task log

The administrator can also view a log of this particular server task by double clicking the particular server task on the Server Task Log page in ePolicy Orchestrator. This log displays only high level information about the users, groups or OUs, and not the detailed log; however, when an LDAP user assigned to **EE: Users** is deleted/disabled from the LDAP server, then the **EE LDAP Server User/Group Synchronization** task log shows the user information of the removed user account.



Server Task Log Details

Server Task Log Information

Name:	safe sync
Source:	Server Task
Start Date:	8/30/12 3:59:57 PM
Duration:	Less than a minute
User Name:	admin
Status:	Completed

Log Messages | Subtasks

8/30/12 3:59:57 PM	Started: Synchronizing LDAP information for [safeboot].
8/30/12 3:59:59 PM	Started: Checking for unreferenced groups
8/30/12 3:59:59 PM	Completed: Checking for unreferenced groups
8/30/12 4:00:00 PM	Started: Adding recursive groups
8/30/12 4:00:00 PM	Completed: Adding recursive groups
8/30/12 4:00:00 PM	Started: Synchronizing groups
8/30/12 4:00:00 PM	Completed: Synchronizing groups
8/30/12 4:00:00 PM	Started: Checking for unreferenced users
8/30/12 4:00:00 PM	Completed: Checking for unreferenced users
8/30/12 4:00:00 PM	Started: Synchronizing users
8/30/12 4:00:02 PM	Completed: Synchronizing users
8/30/12 4:00:02 PM	Completed: Synchronizing LDAP information for [safeboot]. (Endpoint Encryption LDAP server user/group synchonization task)

Figure 3-3 Server task log

Adding users

Select specific OUs, User(s), or Group(s) while assigning users using **Menu** | **Data Protection** | **Encryption Users** | **Actions** | **Endpoint Encryption** | **Add User(s)** option. The Add User(s) page provides three options such as **Users**, **From the groups**, and **From the organizational units** with recursive option for Groups and OUs. You can click on the corresponding **Browse** button and list the Users/Groups/OUs present in the configured LDAP server.

The McAfee ePO server allows the administrator to filter user accounts that can be imported into EEPC/EEMac, based on a portion of LDAP. For example, if the configured LDAP has two major Organizational Units (OUs): OU=My OU and OU=Phils_OU and if only the user accounts from OU=My OU need to be imported then it can be achieved easily using ePO Server.

The **Recursive** option, if selected, adds the users of the sub groups and Sub OUs in the selected groups and OUs.

Figure 3-4 Adding EE users

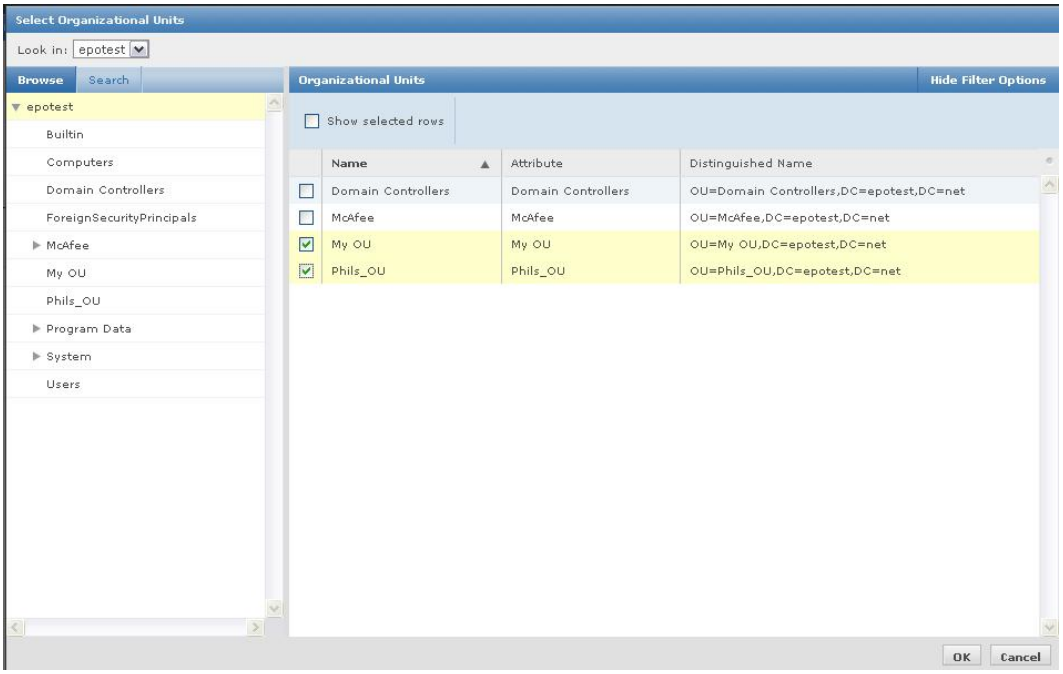


Figure 3-5 Assigning users from OUs

Recommended Product Settings Policy

The Product Settings Policy controls the behavior of the Endpoint Encryption client. For example, it contains the options for enabling encryption, enabling automatic booting, and controlling the theme for the Pre-Boot environment.

You can configure the Product Settings Policies by navigating through **Menu** | **Policy** | **Policy Catalog**, then selecting **Endpoint Encryption 7.0.1** from the Product drop-down list. Select **Product Settings** from the Category drop-down list. Locate the My Default policy and click **Edit Settings**. For more information about individual policy setting, see the *McAfee Endpoint Encryption - 7.0 Patch 1 Product Guide*.

Table 3-1 Recommended Product Settings Policies

Policy Options	Recommendations
General Tab	• **Enable Policy** — Leave this option checked (enabled). This policy should be enabled to activate Endpoint Encryption on the client system. This option needs to be disabled to uninstall Endpoint Encryption from the client. • **Logging Level** — Set the required logging level. To overwrite the logging level defined in ePolicy Orchestrator, the **LoggingLevelOverride** registrykey needs to be set on the client system. • **None** — Does not create any log for the client system managed by McAfee ePO. • **Error** — Logs only error messages. • **Error and Warnings** — Logs the error and warning messages. • **Error, Warnings, and Informational** — Logs the error and warning messages with more descriptions. • **Error, Warnings, Informational and Debug** — Logs the error, warning, and debug messages. We recommend that you enable this option only when you require extended logging for troubleshooting purposes. Try not to enable this option for standard usage because it might impact the performance. • **Allow temporary automatic booting** — Enable this option that allows the administrator to run the temporary autoboot tool on the client system, so it can automatically boot without prompting for a Pre-Boot Authentication. • **Expire Uninitialized Users** — Leave this option checked (enabled). Allows the administrator to control and manage the users who have not logged on to the client system. Enabling this option forces the user account, which is not initialized, to expire after a number of hours as set in the policy. This feature allows you to control access to client systems by preventing unauthorized access using uninitialized user accounts. Make sure to note that this policy is not applicable to EFI systems. • **Allow Machine Information Collection** — Leave this option checked (enabled). Enabling this option allows the user to collect client system details such as the list of assigned users, policy settings, recovery, and Endpoint Encryption Status. After enabling this option, the user will see a new button Save Machine info in: • Windows — **McAfee Agent Tray | Quick Settings | Show Endpoint Encryption Status** • Mac — **Encryption icon** on the menu bar that is present on the desktop of the client. You can click this button and save the text file for later reference.
Encryption Tab	• **Encrypt** — **All Disks** is a recommended option (The **None** option does not initiate the encryption). The All disks except boot disk option, which encrypts all disks except the boot disk is not a recommended option. • **Selected Partitions** — Allows you to select the required partitions of the client system and select them to be encrypted. You can select the required partitions by

Table 3-1 Recommended Product Settings Policies *(continued)*

Policy Options	Recommendations
	specifying the Windows or Mac drive letters/volume names. Partition level encryption is not applicable to client systems using OPAL encryption. Do not assign a drive letter to the Windows 7 hidden system partition on your client system. Doing so, will stop the EEPC software from being activated on the client system. The **Encryption type** options such as **None**, **All disks except boot disk**, and **Selected partitions** are not applicable to self-encrypting drives in Opal mode Make sure that you select the required encryption type, as appropriate. Policy enforcement might fail on client systems if you select an unsupported encryption type. This table also lists the encryption providers (PC Software and PC Opal or Mac OS X) available with the software. You can change and set the encryption priority by moving the encryption provider rows up and down, as appropriate. By default, software encryption will be used on both Opal and non-Opal systems in this version of EEPC. To ensure that Opal technology is chosen in preference to software encryption, we recommend that you always set Opal as the default encryption provider, by moving it to the top of the list on the Encryption Providers page. This ensures that Opal locking will be used on Opal drives. When enforcing a policy to a group of Mac OS X or PC systems, we recommend that you select Mac OS X Software or PC Software first in the priority list.

Table 3-1 Recommended Product Settings Policies *(continued)*

Policy Options	Recommendations

Log On Tab	• **Enable automatic booting** — Leave this option unchecked (disabled). If you enable this feature, the client system does not have the PBA. This is normally referred as Autoboot mode. It could be useful to enable this option when the administrator needs to manage the autobooting scenarios. There are multiple scenarios where you can have this option enabled or disabled. For instance, during rollout to minimize the end user impact or during patch cycles to allow the patches to be installed and the reboots to happen without end user intervention. However, it is the responsibility of the administrator to decide on when to enable or disable this option.
	
	If you enable this option, be aware that the McAfee Endpoint Encryption software does not protect the data on the drive when it is not in use.
	
	• **Disable and restart system after 3 (1-10) failed logons or unlocks (Windows only, Vista onwards)** — It is advisable to enable this option, if you had enabled the **Enable automatic booting** option. On enabling this option, the autoboot of the system is disabled after a specific number (defaulted to 3 or specify from 1-10) of failed Windows logons.
	
	• **Do not display previous user name at log on** — Leave this option checked (enabled). On enabling this option, the client system does not display the user name of the last logged on user automatically on all EEPC logon dialog boxes.
	
	• **Enable on screen keyboard** — Leave this option checked (enabled), especially for tablets or on screen mouse device systems. This option enables the Pre-Boot On-Screen Keyboard (OSK) and the associated Wacom serial pen driver. When this option is enabled, the pen driver finds a supported pen hardware (Panasonic CF-H1 and Samsung Slate 7) and displays the OSK.
	
	If you do not select this option, the BIOS will use mouse emulation. In such a situation, the BIOS will treat the digitizer as a standard mouse, which might lead to the cursor being out of sync with the stylus on USB connected Wacom pen digitizers. Please note that this feature is not applicable to EEMac.
	
	• **Always display on screen keyboard** — Forces the Pre-Boot to always display a clickable on-screen keyboard regardless of whether the pen driver finds suitable hardware or not.
	
	Note that this is only valid for BIOS based hardware. On UEFI, you should note that the digitizer is managed by the UEFI software, so the UEFI implementation needs to contain drivers for the digitizer.
	
	• **Add local domain users (and tag with 'EE:ALDU')**
	  • **Disabled** — Selecting this option does not add any local domain users to the client system.
	  • **Add all previous and current local domain users of the system** — On selecting this option, any domain users who have previously and are currently logged on to the system, are able to authenticate through the Pre-Boot, even if the administrator has not explicitly assigned the user to the client system.
	  • **Only add currently logged on local domain user(s); activation is dependent on a successful user assignment** — Leave this option selected (enabled). On selecting this option, only the domain users who are logged on to the current Windows session, are added to the system

Table 3-1 Recommended Product Settings Policies *(continued)*

Policy Options	Recommendations

and hence EEPC is activated, even if the administrator has not explicitly assigned the user to the client system.

If you select this option, at least one user should be added to the client system for a successful EEPC or EEMac activation on the client. The activation doesn't happen until a user logs on to Windows or Mac OS X as domain user. This domain should have been registered in McAfee ePO.

- **Enable Accessibility** (Windows BIOS systems only) — Leave this option selected (enabled). This option is helpful to visually challenged users. If selected, the system gives a beep as a signal when the user moves the focus from one field to the next using mouse or keyboard, in the Pre-Boot environment. The USB audio functionality allows the visually impaired users to listen to an audio signal (spoken word) as a guidance when the user moves the cursor from one field to the next, in the Pre-Boot environment. The USB speakers and headphones can be used to listen to the audio signal.

  This is not applicable to EEMac.

- **Disable pre-boot authentication when not synchronized** — Leave this option checked (enabled).On selecting this option, the user is blocked from logging on to PBA in the client system, if the client system is not synchronized with the McAfee ePO server for the set number of days. When the user is blocked from logging on to PBA, the user should request the administrator to perform the Administrator Recovery to unlock the client system. This allows the client system to boot and communicate with the McAfee ePO server.

  The client system will continue to block the user from logging on to the system until the synchronization with ePolicy Orchestrator happens. This is specially useful to prevent unauthorized access to laptops that have been misplaced, lost or stolen.

- **Get username from token** — Leave this option checked (enabled). On selecting this option, the available user information on the client system is automatically retrieved from the inserted smartcard; hence the Authentication window does not prompt for a username. The user can then authenticate just by typing the correct PIN.

  You need to enable the matching rules that are required for matching smartcard user principle name (UPN) with EEPC usernames.

  This feature is supported on the Gemalto .Net V2+ tokens, and PIV and CAC tokens. This is not applicable to EEMac.

  - **Match certificate user name field up to @ sign** — Match the certificate user name up to the @ sign of the user name. For example, if the UPN is SomeUser@SomeDomain.com and the EEPC user name is SomeUser, a match is found.
  - **Hide user name during authentication** — On selecting this option, the EEPC user name does not appear in the Authentication window.

- **Enable SSO** — Leave this option checked (enabled).

  This is not applicable to EEMac.

  - **Must match user name** — Leave this option checked (enabled). This option ensures the SSO details are only captured when the user's Endpoint Encryption and Windows user names match. This ensures that the SSO data captured is replayed for the

Table 3-1 Recommended Product Settings Policies *(continued)*

Policy Options	Recommendations
	user for which it was captured. When you select the Enable SSO option, the Must match user name option is also enabled by default. • **Using smart card PIN** — Leave this option checked or unchecked based on whether the eToken/smart card is used or not. This option allows EEPC to capture the smart card PIN for SSO. • **Synchronize Endpoint Encryption Password with Windows** — Leave this option checked (enabled). If selected, the Endpoint Encryption password synchronizes to match the Windows password when the Windows password is changed on the client system. For example, if users change their password on the client, the Endpoint Encryption password is also changed to the same value. • **Allow user to cancel SSO** — Leave this option checked (enabled). This option allows the user to cancel the SSO to Windows in Pre-Boot. When this option is enabled, the user has an additional checkbox at the bottom of the Pre-Boot logon dialog box. • **Lock workstation when inactive** — Leave this option unchecked (disabled). The client system is locked when it is inactive for the set time.
Recovery Tab	• **Enabled** — Leave this option checked (enabled). This is enabled by default to make sure that the recovery is possible at any stage of the Endpoint Encryption management. • **Key size** — After consulting with your IT security, set the key size to the size adequate for your organization requirements. This refers to a recovery key size that creates a short Response Code for the recovery. • **Message** — You could use this option to display your HelpDesk phone number or instruct the user to use the self recovery option. • **Allow users to re-enroll self-recovery information at PBA** — Leave this option checked (enabled) only when required. On enabling this option, the client user's self-recovery details can be reset, then the user has to enroll the self-recovery details with new self-recovery answers. Before resetting the self-recovery questions on the client system, make sure that you have enabled the **Enable Self Recovery** option under **User Based Policy | Self-Recovery**. Once this option is enabled, the Pre-Boot Authentication (user name) screen will have a new checkbox **Reset self-recovery**. On selecting the **Reset self-recovery** checkbox, the user will be prompted for a password and then the self-recovery enrollment. Only initialized users can reset their self-recovery details.

Table 3-1 Recommended Product Settings Policies *(continued)*

Policy Options	Recommendations
Boot Options Tab (Windows only)	• **Enable Boot Manager** — Leave this option unchecked (disabled). Enabling this option activates the built in pre-boot partition manager. This allows you to select the primary partition on the hard disk that you wish to boot. Naming of the partition is also possible with the boot manager. The time out for the booting to start can also be set. • **Always enable pre-boot USB support** — Leave this option checked only when needed. (enabled). Forces the Endpoint Encryption Pre-Boot code to always initialize the USB stack. USB audio functionality allows the visually impaired users to listen to an audio signal (spoken word) as a guidance when the user moves the cursor from one field to the next, in the Pre-Boot environment. The USB speakers and headphones can be used to listen to the audio signal. You will notice an improper synchronization of the mouse cursor and the stylus on USB connected Wacom pen digitizers. To avoid this, make sure to enable this option. • **Always enable pre-boot PCMCIA support** — Leave this option unchecked (disabled) unless you require support for PCMCIA devices in Pre-Boot. • **Graphics mode** — Automatic. Allows you to select the screen resolution for a system or a system group.
Theme Tab	It is better to have the default option enabled as it is simple to deploy and manage.
Out-of-Band Tab (Windows only)	**Enable at PBA**— Enable this option to enable the EEPC out-of-band management features through policies and then perform actions on Intel® AMT provisioned client systems. You can enable this option only if you have installed the **Endpoint Encryption : Out Of Band Management** extension in McAfee ePO.

Table 3-1 Recommended Product Settings Policies *(continued)*

Policy Options	Recommendations
Encryption Providers Tab (Windows only)	• **Use compatible MBR** — Leave this option unchecked (disabled). This causes EEPC to boot a built-in fixed MBR instead of the original MBR that was on the system after pre-boot logon. It is used to avoid problems with some systems that had other software that runs from the MBR and no longer work if EEPC is installed. • **Fix OS boot record sides** — Leave this option unchecked (disabled). Some boot records report an incorrect number of sides. Selecting this option fixes this on the client system. This is available only when you install the EEPC extension. • **Use Windows system drive as boot drive** — Leave this option unchecked (disabled). This is for maintaining the compatibility with some systems where the disk 0 is not the boot disk. Selecting this option forces the users product to assume that the boot disk is the one that contains the Windows directory but not disk 0. • **Enable Pre-Boot Smart Check (BIOS-based systems only)** — Leave this option checked (enabled) only when needed. When you enable this feature, it modifies the EEPC activation sequence and creates a pre-activation stage, where a series of hardware compatibility checks are performed prior to actual activation and subsequent encryption to successfully activate EEPC on platforms where BIOS issues might exist. This feature is available only for BIOS systems using PC software encryption, and is not available for UEFI or Opal systems. There will be several reboots of the client system before the Smart Check is completed. • **Force system restart once activation completes** — Leave this option checked only when needed. (enabled). This option is selected by default when you select the **Enable Pre-Boot Smart Check (BIOS based systems only)** option to restart your system after activation.
PC Opal (Windows only)	This option requires all the drives in your client system to be Opal for the PC Opal encryption provider to be activated.
Mac Software	• **Allow software updates** — Allows the user to perform the software update for Mac OS X from the Apple update server. • **Allow software updates but warn users**—Leave this option checked (enabled). Allows the user to perform the software update for Mac OS X from the Apple update server. However, the following notification is displayed before the software update is performed: Applying Operating System or Firmware updates to systems with McAfee Endpoint Encryption for Mac installed can potentially cause problems. For more information, refer to the https://kc.mcafee.com/corporate/index?page=content&id=KB68921 KnowledgeBase article. • **Block software updates**—This is optional because the administrator can block software updates as per the requirements.

Recommended User-Based Policy Settings

The User-Based Policy controls the parameters for Endpoint Encryption user accounts. For example, it contains the options for selecting a token type (including password and smartcard) and password content rules.

You can configure the User Based Policies by navigating through **Menu** | **Policy** | **Policy Catalog**, then selecting **Endpoint Encryption 7.0.1** from the Product drop-down list.

Select User Based Policies from the **Category** drop-down list. Locate the **My Default** policy and click **Edit Settings**. For more information about individual policy setting, see the *McAfee Endpoint Encryption - 7.0 Patch 1 Product Guide*.

User Based Policies in Endpoint Encryption

A requirement of EEPC 7.0 Patch 1 is that you need to specify which groups of users are allowed or not to use the Policy Assignment Rules. The allowed users get their required User Based Policies. Users that are not allowed to use the Policy Assignment Rules inherit the default User Based Policies assigned to the system.

In EEMac, the User Based Polices are assigned just like Product Setting Policies. A single UBP is enforced to all the users in EEMac.

Enforce the desired user-based policy to a user assigned to a client system by enabling the **Configure UBP enforcement** option.

It is always better to assign the User Based Policies at the system level or branch level if possible, rather than assigning using the Policy Assignment Rules. However, you can use the Policy Assignment Rule option, if required, for assigning different policies to different users.

Table 3-2 Recommended User Based Policy Settings

Policy Options	Recommendations

Authentication Tab	• **Token type**: Select **Password only**. There are a number of other tokens that can be effectively used for your authentication as required. However, the Password only token is as strong as any other token that you could configure.
	• **Certificate rule**
	  • **Provide LDAP user certificate** — Leave this option checked (enabled).
	  • **Use latest certificate** — Leave this option checked (enabled).
	  The **Certificate rule** options are not active if **Password only** token is selected.
	• **Logon hours** — You could enable and set the logon day and time-line as required. It is better to have this disabled if you do not have a specific requirement.

Password Tab	• **Change Default Password** — Leave this option checked (enabled). This allows you to set a default password that is different from the default product setting. All new users are prompted to change the default password during user initialization.
	  • **Do not prompt for default password** — Leave this option checked (enabled). When enabled, users are prompted to type in their EEPC password without having to remember a common default password. If you enable this option, you don't have to enable the **Change Default Password** option.
	• **Password Change** — Disable all of these settings as you would be using SSO and don't want to cause conflict with Windows password requirements.
	  • **Enable Password history** — Leave this option checked (enabled) to prevent users from reusing passwords unless your security policy exempts users from using new passwords.
	  • **Prevent change** — Leave this option unchecked (disabled).
	  • **Require change after ____ days (1-366)**—Leave this option unchecked (disabled).
	  • **Warn user _____ days before password expiry (0-30)**—This is disabled by default when you disable the **Require change after ____ days (1-366)** option.
	• **Incorrect Passwords**
	  • **Timeout password entry after ----invalid attempts (3-20)** — Set required number of password invalid attempts.
	  • **Maximum disable time ------ minutes (1-64)** — This is disabled by default when you disable the **Timeout password** option.
	  • **Invalidate password after ------ invalid attempts** — Leave this option checked (enabled).

Table 3-2 Recommended User Based Policy Settings *(continued)*

Policy Options	Recommendations
Password Content Rules Tab	• **Password length** — Use default. • **Enforce password content** — Use default. • **Password content restrictions** — Use default or enable restrictions for better password strength.
Self-Recovery Tab	• **Enable self-recovery** — Leave this option checked (enabled). • **Invalidate self recovery after No. of invalid attempts**: Enable and set the number of attempts to a number that does not abruptly lock out the Self Recovery. • **Questions to be answered** — Can be set to 3. This can give you the required security without giving the user a lot of pain of keying in the characters. However, it is up to the administrator to decide this number depending on the requirement. • **Logons before forcing user to set answers** — Set this to 0. This makes sure the users set the answers during the user initialization. • **Questions** — Use the default ones or configure the questions as required.

Checklist for using Intel® AMT and EEPC

The Intel® AMT out-of-band feature within EEPC 7.0 Patch 1 provides system actions that include **Out Of Band - Remediation**, **Out Of Band - Unlock PBA**, and **Out Of Band - User Management**.

For more information about these actions, see the Configure the Out Of Band - Remediation feature, Configure the Out Of Band - Unlock PBA feature, and Configure the Out Of Band - User Management feature sections in the *Endpoint Encryption 7.0 Patch 1 Product Guide*. These actions are available on the McAfee ePO console only after installing the EEDeep extension.

You must install the McAfee Deep Command product extensions before installing the EEDeep extension.

For more information about requirements for configuring your Intel® AMT systems, see the ePO Deep Command Product Guide.

Preparation for using Intel® AMT with EEPC

- Make sure that the client system has been provisioned for Intel® AMT.
- The Deep Command software has been installed and its policies have been configured correctly.
- Make sure that CILA/CIRA policies have been applied and CILA/CIRA has not been disabled at Deep Command Server Settings.
- Make sure that the client system is managed by McAfee ePO and the Intel® AMT policy has been successfully deployed.
  - Check the AMTService.log file to verify that the Intel® AMT policy is enforced correctly.
  - At this point, you should be able to power the system on into BIOS to verify this.
- Make sure that you have installed the EEAdmin, EEPC and EEDeep extensions.
- Make sure that you have configured the EE Product Settings policy for out-of-band features and sent to the client system.

- Deploy the EEAgent and EEPC packages to the client system.
- Activate EEPC and restart client system.

Best practices and recommendations for using Intel® AMT and EEPC

- Enable CIRA only when it is necessary for the security requirements of your organization.
- Limit the usage of EEDeep unlock feature during wake-and-patch cycles to the smallest time/number of reboots.
- While performing any out-of-band action, do not power off or disconnect the client system from network until the system successfully boots into Windows.
- Note that the time-based out-of-band actions, for example unlock on schedule, are based on the clock on the server. They are not based on the local time of the client system even if it is on another time zone.
- Out-of-band: remediation — Always allow **Automatic** disk image to be used when possible.
- Out-of-band: user management — Even though password policy is not enforced on the temporary password, make sure to follow the enterprise password policy for setting the temporary password.

Phased deployment strategies

Endpoint Encryption deployment (first time installation) can be done in various phases with different policy settings for different corporate environments. A model policy setting is explained in the recommended policy settings sections.

Phased deployment (first time installation)

There can be a number of scenarios where the PBA creates challenges during the Endpoint Encryption deployment. For a safe and smooth deployment and activation process, you can easily create different sets of EEPC/EEMac system policies and do the deployment in various phases.

During the first time installation, it is a best practice to create the first set of policy settings with **Encryption** set to **None** and **Automatic Booting** enabled. You can create a second set of policy settings which enables the encryption and the PBA.

When the first set of policies is in use, the client systems are unprotected.

High level process

- After deploying the Endpoint Encryption packages, create an Endpoint Encryption system policy with the following settings:
  - Select the encryption option as **None** under **Encryption tab** | **Encrypt**.
  - Enable the **Enable Automatic Booting** option under Log On tab | Endpoint Encryption.
  - Enable **Add local domain users** option under Log On tab | Endpoint Encryption.
- Enforce this policy to the client systems. This activates Endpoint Encryption, but encrypts no disks and requires no authentication.
- You can now configure the second set of policy with the required encryption option other than **None** and autobooting disabled.
- Use the automatic booting policy as the default. In this mode, the Add Local Domain Users feature captures all Windows domain accounts that access the system. These accounts are added as valid Pre-Boot enabled accounts to be used in the Pre-Boot environment.

- Create a query in ePolicy Orchestrator to find all systems that need to stop autobooting and assign the second policy to these systems.
- Send an agent wake-up call from ePolicy Orchestrator to apply the policy with Pre-Boot Authentication to all required systems.
- The systems will start with PBA as and when the new policy is received.

This phased deployment will temporarily enable automatic booting and then when the query is run, it enables the Pre-Boot Authentication policy. This ensures that Endpoint Encryption gets activated when the system is in the field and ensures that the end user's account gets added as a valid Pre-Boot account before encrypting and activating PBA.

This kind of phased deployment can be very useful as and when the administrator meets with challenges such as patching cycles, re-imaging process, deploying product and managing other autoboot scenarios.

Perform phased deployment in batches of systems from the System Tree.

Auto booting

Auto Booting (Enable Automatic Booting) is used by administrators for re-imaging process, patching cycles, and product deployments. Many software installation packages require one or more restarts of the target computer, and autobooting automatically authenticates without user or administrator intervention. The administrator can define a window of time-line during which autobooting remains active.

The autoboot feature terminates when the defined time-line window has elapsed.

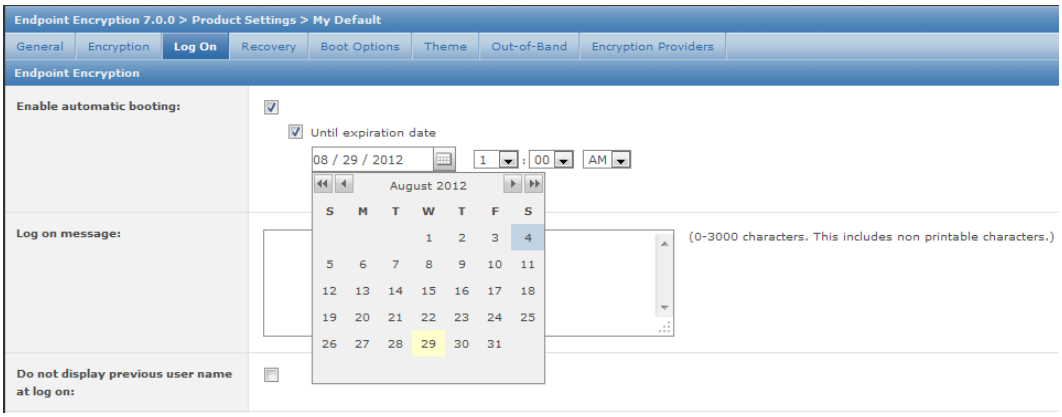


Figure 3-6 Configure auto booting

Since this policy setting temporarily bypasses the normal logon process for Endpoint Encryption installed systems, computers receiving this policy will be vulnerable while Autobooting remains active. To minimize the risk, make sure that you carefully review the inclusive dates and times that Autobooting remains active before deploying this policy.

4 Deployment and activation

The purpose of this section is to provide guidance with troubleshooting on why the Windows or Mac operating system will not start; encrypted systems do not allow access to the operating system until PBA is completed.

Administrators should be mindful that fixing certain Windows or Mac problems on an encrypted system may require extra caution in the event that the registry must be edited or a driver should be modified.

Traditional recovery procedures will also change on a system encrypted with Endpoint Encryption 7.0 Patch 1. For example, the entire disk is encrypted which means the file systems and disks are accessible only when the Pre-Boot Authentication is complete.

The EETech User Guide provides instructions on how to create a customized pre-installation disk with the EEPC/EEMac drivers loaded. This disk allows the administrator to access an encrypted hard drive or Opal drive to update the drivers or the registry. For more information, refer to the EETech User Guide.

Booting the Endpoint Encryption installed client requires the physical presence of the client user to supply credentials at the Endpoint Encryption PBA page.

To gain access to an encrypted computer, the user must always enter credentials at the PBA screen. It is important that this change in client operation be understood and adopted into your operating procedures. Administrators should be mindful of dispatching drivers/service packs to client systems as the system will inevitably require reboot after install.

The **Enable Automatic Booting** option in the **Product Settings Policy** allows access to the Endpoint Encryption installed systems without actually having to authenticate through PBA. However, it is the administrators' responsibility to ensure that system security is not compromised if this option is selected, as Autoboot effectively removes system security. Alternatively, you can also use the OS refresh process to keep the systems secure with minimal user intervention.

Contents

- *Basic preparations and recommendations*
- *High level process of the installation*
- *Client task to deploy the EEAgent and Endpoint Encryption packages*
- *Add group users*
- *Endpoint Encryption activation sequence*
- *Activate Endpoint Encryption using Add local domain users*
- *Skip Unused Sectors*

Basic preparations and recommendations

The following recommendations will make sure that your data is protected during and after the encryption process.

As with any roll out and deployment, it is advisable to back up the system before you encrypt it, and perform regular backups

It is good practice to back up the system before installing Endpoint Encryption to ensure data is not lost in the unlikely event a problem occurs. The EETech recovery tools can also be used to decrypt and recover any unbootable disks. Please refer to the EETech User Guide for more information.

When upgrading EEPC the Mfeepehost service must not be stopped either manually or by third party software since this can cause problems. Also note that during an upgrade the system must be kept powered on until the software (both Host and Admin portions) complete installing.

CHKDSK /r Clean up the disk before you encrypt it

Hard disks that are damaged, or have a high number of undiscovered bad sectors, may fail during the full disk encryption process. Run a **CHKDSK /r** command prior to installing EEPC to make sure the disk is healthy. Optionally, run the OEM diagnostic tools to make sure that all other HW components are working correctly.

Use the Disk Utility application in Mac to verify and repair any disk errors on Mac client systems.

Understand the supported tokens/readers for EEPC/EEMac

Make sure that the supported reader drivers are installed in your client system before trying to install Endpoint Encryption. Make sure to obtain the correct drivers from the manufacturer website and review their release notes to avoid any known issues with the tokens or readers. The supported tokens and readers are listed in these KB articles:

- Supported Readers used for authentication in McAfee Endpoint Encryption for PC 7.x: https://kc.mcafee.com/corporate/index?page=content&id=KB76590
- Supported Tokens used for authentication in McAfee Endpoint Encryption for PC 7.x: https://kc.mcafee.com/corporate/index?page=content&id=KB76589
- Supported Readers used for authentication in McAfee Endpoint Encryption for Mac 6.x and 7.x: https://kc.mcafee.com/corporate/index?page=content&id=KB75182
- Supported Tokens used for authentication in McAfee Endpoint Encryption for Mac 6.x and 7.x: https://kc.mcafee.com/corporate/index?page=content&id=KB75183

Maintain separate test and production clients

Enterprise administrators are advised to maintain separate test and production environments. Modification to the production server should be limited. Use the test system to test software updates, driver updates and Windows Service Packs prior to updating the production systems.

Build and test recovery tools

The administrator needs to be aware that there will be changes to the normal client boot process due to installing EEPC. Administrators are advised to:

- Create and test the customized EETech WinPE V1 or V3 or V4 (for UEFI systems) Disk with EEPC drivers installed.
- Create and test an EETech Standalone Boot disk.

Run a pilot test of software compatibility

We recommend that you run a pilot test of EEPC on a client system. This will make sure that EEPC is not in conflict with any encryption software on the client computers before rolling out to a large number of clients. EEGO can be a valuable tool to detect the presence of third party encryption software that may prevent activation or create further issues with EEPC.

This is particularly useful in environments that use a standardized client image.

Administrators should also run performance testing during the pilot test.

McAfee professionals did not come across any performance related issues with EEPC during our own testing, however, this may vary depending upon the processor, memory, and drivers.

Do a phased deployment

An occasion may arise when the PBA creates challenges during deployment. For a successful deployment and activation, you can create a different set of EEPC system policies and deploy in phases enabling the **None** option under **Encrypt** and **Enable Automatic Booting** option under **Log on** tab. Create deployment tasks and deploy EEPC to systems arranged in groups or batches in the **System Tree**. You can also base it on a specific tag in ePolicy Orchestrator.

Add user to the client system

You should add at least one user to the client system for EEPC to activate on the client.

Perform disk recovery on decrypted disks

Wherever possible, as a best practice, if you need to perform any disk recovery activities on a disk protected with McAfee EEPC, we recommend that you first decrypt the disk. For more information about decrypting the EEPC installed system, see *McAfee Endpoint Encryption - 7.0 Patch 1 Product Guide* and the *McAfee EETech User Guide*.

Automatic Repair should be disabled in Windows 8 systems

Automatic Repair of an encrypted disk in Windows 8 systems may destroy the encrypted operating system files without any notification and cause permanent boot problems. However, previous versions of Windows displays confirmation message before starting the repair. Windows 8 launches into Automatic Repair immediately a problem is detected, leaving little scope to prevent destruction of encrypted data.

To disable Automatic Repair, run this command from an administrative command prompt:

```
bcdedit /set {current} recoveryenabled No
```

Educate the client user with the Password/Token/PIN secrecy

Educate your client users to understand they are responsible for the security of their password, PIN, or token details. Encourage them to change their password, or request a new PIN, if they feel that it may have been compromised.

Make sure password strength is sufficient

Make sure that your password policy is strong enough for your requirements.

High level process of the installation

This section lists the steps and considerations involved in Endpoint Encryption deployment and activation.

This procedure is explained in more detail in the *McAfee Endpoint Encryption - 7.0 Patch 1 Product Guide*.

Task

1. Install the EEPC/EEMac extensions into ePolicy Orchestrator. Check for the correct and latest version of the extension. Install EEAdmin extension first then EEPC.
2. Check in the EEPC/EEMac packages to ePolicy Orchestrator. Check for the correct and latest version of the EEAdmin and EEPC packages.
3. Register your LDAP Server. Check for the correct domain and Server IP address of your LDAP server configured.
4. Create **EE LDAP Server User/Group Synchronization** task and schedule it to run. Check for the correct format of the user attributes while scheduling the task.
5. Modify the Product Settings and User-Based Policies, as appropriate. Plan and verify the policy settings for your organization's requirements.
6. Add a user to the client system. Decide whether to add the users manually in ePolicy Orchestrator or to add users using the **Add local domain user** option present under the **Product Settings Policy**. At least one user must be assigned to each client in order to activate EEPC on it.
7. Create a client task to deploy the EEPC/EEMac components to the client systems. Make sure that you deploy the packages in the right order (EEAgent then EEPC/EEMac).
8. Test for successful deployment, activation and encryption on targeted endpoints. Make sure to make use of the reporting facilities available in the ePolicy Orchestrator management software.

Client task to deploy the EEAgent and Endpoint Encryption packages

We recommend that you create a new system group in ePolicy Orchestrator for Endpoint Encryption deployment. Name it EEPC/EEMac Test Systems or EEPC/EEMac Production Systems, respectively, for example.

Do not create the deployment task at the **My Organization** level of the **System Tree**. Select a group in the **System Tree**, go to the **Client Tasks** tab and create the deployment task.

Importing systems from Active Directory to ePolicy Orchestrator

McAfee ePO provides an **AD Synchronization/NT domain** task to synchronize ePolicy Orchestrator with the configured Active Directory. This option allows you to map the ePolicy Orchestrator **System Tree** structure with a registered AD. Using this option, you can import and effectively manage large numbers of systems in ePolicy Orchestrator.

This option works only with Active Directory.

Refer to the product documentation for your version of McAfee ePO, for detailed procedures on how to import systems from Active Directory to ePolicy Orchestrator.

Order of the EEAgent and Endpoint Encryption deployment

It is not mandatory to have two different tasks for the product deployment. You can create one single task to deploy both packages, but don't forget that they need to be deployed in the right order. The EEAgent package should be followed by the EEPC/EEMac package.

If you configure to deploy the EEPC/EEMac package followed by the EEAgent package then the client system restarts in the middle as required and the EEAgent would never get deployed.

So, it is always better to execute the deployment using a single task wherein you need to deploy the EEAgent package first then the EEPC/EEMac package.

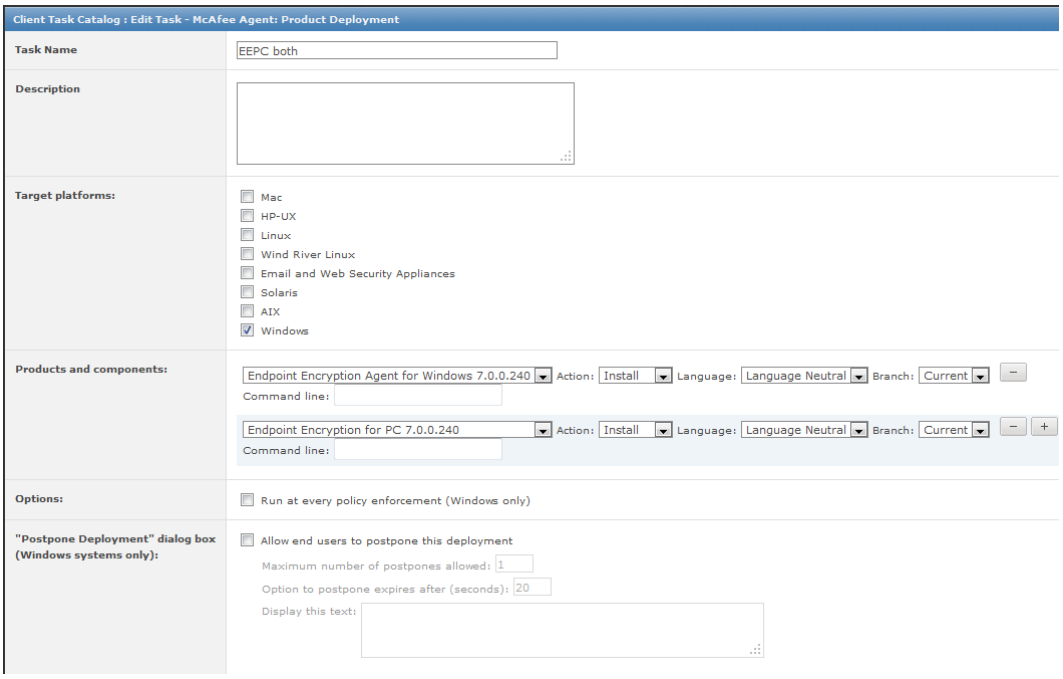


Figure 4-1 EEAgent and EEPC packages deployment

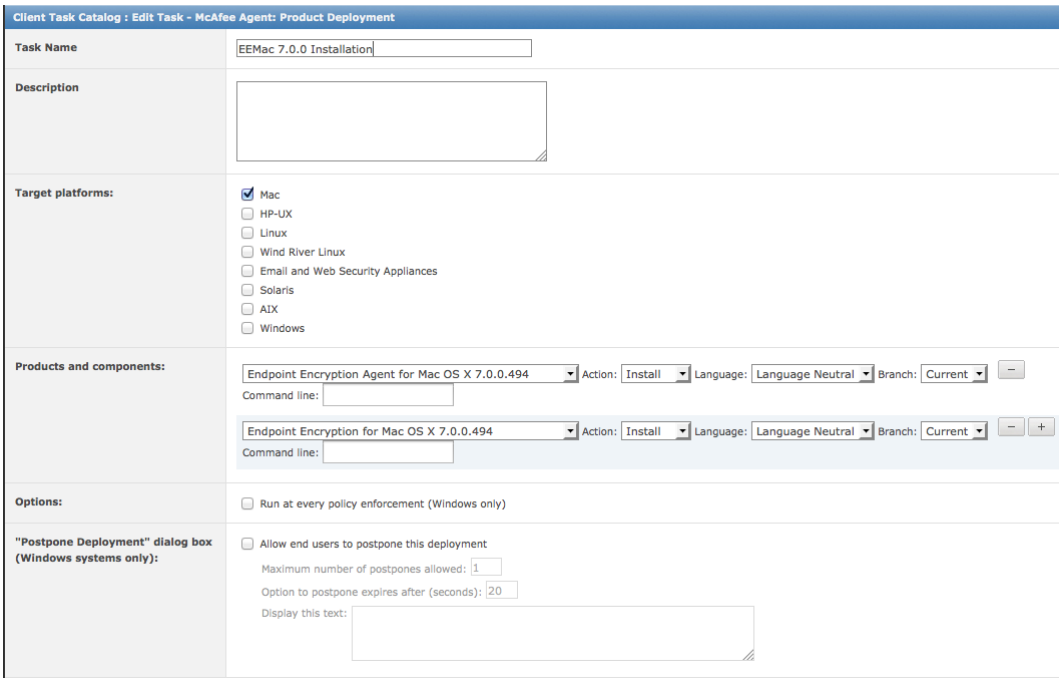


Figure 4-2 EEAgent and EEMac packages deployment

You can also create two separate tasks to deploy the packages, providing you wait for the first deployment (EEAgent) to complete before deploying the second package. You can also verify the completion of the EEAgent deployment, before deploying the EEPC/EEMac package, by creating and executing a customized query from the McAfee ePO server. If the EEPC/EEMac package is deployed first, you can run the EEAgent task and deploy it later.

End user experience

The deployment task pushes both the Endpoint Encryption Agent and the EEPC/EEMac components to the selected systems. The installation is silent, however, the user is prompted to restart the client when the EEPC/EEMac component install is complete. It is important that the user restarts the client PC when prompted. If this does not happen, EEPC/EEMac will not activate.

When the EEMac product is active on the client system, you should not perform any disk partitioning activities.

Add group users

Group Users are the Endpoint Encryption user accounts that are allocated to every encrypted system. They are typically administration accounts used for troubleshooting and supporting the client in a given group.

If you choose to add a Group or an Organizational Unit (OU), you will not see the individual user names. Instead, you will see the entire Domain Name of the Group or Organizational unit.

If you do not follow the recommendations on **Change default password** and **Do not prompt for default password** options, then all Endpoint Encryption user accounts, including Group User, accounts get assigned the default password upon creation. If the default password is not changed in the User-Based Policies then use **12345** as the default password for the first time you log on with these user accounts.

If you want the system to capture the user's credentials automatically without having to make them use a default password on PBA, enable the **Do not Prompt for default password** option under **User Based Policies** | **Password**.

Users

To access the data on an encrypted computer, the user must go through the PBA. If the **Enable Auto Booting** option is not enabled then the client user is presented with the PBA screen when the system is restarted after activating Endpoint Encryption.

During the first Pre-Boot after activation, the user needs to initialize the user account with the default password and enroll for the self recovery if this feature has been enabled in the policy.

Make sure that at least one manually added user is assigned to the client system. For example, this could be an admin user assigned to all systems.

During the initialization process, users will set up their Pre-Boot credentials to unlock the disk. Only the assigned users from a registered LDAP server will be accepted by Endpoint Encryption PBA.

At least one Endpoint Encryption user is required to be assigned to Endpoint Encryption on each client; this could be an administrative user.

Add local domain users

This option automatically adds the previously logged in domain users to the client system, so that administrators don't have to manually assign users to the client systems in the ePolicy Orchestrator console.

This option can be enabled as and when needed through the Endpoint Encryption Product Settings Policies (**Menu** | **Policy** | **Policy Catalog** | **Endpoint Encryption 7.0.1 (Product Settings)** | **Log on tab** | **Add local domain users**).

When enabled, the EEAgent queries the client system for the currently/previously logged on domain users to the client. The EEAgent will then send the collected data to the McAfee ePO server. These users will then be assigned to the client system.

We recommend that you have this option enabled, so that you will always be able to authenticate to the Pre-Boot of the client without having to manually assign the users to the client system in the ePolicy Orchestrator console. However, this is a responsibility of the administrator to decide whether this is required or not depending on corporate requirements.

Prerequisites

The following prerequisites are required to add the local domain users to the Endpoint Encryption client systems:

- The McAfee Agent package is deployed.
- The McAfee EEAgent package is deployed to the required client systems.
- The McAfee EEPC/EEMac package is deployed to the required client systems.
- Registered Active Directory is added and configured correctly.

  The **Add local domain users** option is supported with Active Directory only.

- An automated **EE LDAP Server User/Group Synchronization** task should be scheduled and run.
  - This task is used to map Active Directory attributes to the Endpoint Encryption settings. This is required for every Registered LDAP server that is to be used with Endpoint Encryption.
- Client systems should be using Active Directory for authentication.
  - These domain users must be previously or currently logged in users.

At the client side

The **Add local domain user** option is processed during the next agent to server communication. If this option is enabled in the policy settings, the EEAgent queries the client system for the domain users who have logged on to the client. The EEAgent will then send the collected data to the McAfee ePO server.

The data that is transmitted back will be a list of user names and the domain names. Local Domain users are detected by examining the Windows registry which has the profile list. This list provides the list of users who have logged in to the system.

At the server side

When the EE Admin receives a message for adding local domain users, it executes the following steps.

- It attempts to find the domain name that the user belongs to. This is done by querying the Registered Active Directory that is configured with the automated **EE LDAP Server User/Group Synchronization** task.
- If a registered LDAP server is found then it matches the domain name of the user. An LDAP query is performed and attempts to find an LDAP node with a **samaccountname** that matches the user name.

If the user name is found then it will be assigned to the corresponding client system. You can query the added users by using the **View Users** option under **Menu** | **Data Protection** | **Encryption Users** | **Actions** | **Endpoint Encryption** | **View Users**.

Endpoint Encryption activation sequence

When the EEAgent and EEPC/EEMac packages are successfully deployed, the users will be prompted to restart their system.

The restart can be canceled, however, Endpoint Encryption will not become active on the client until the restart has occurred. Also note that hibernation and using new USB devices will be impaired until a restart is issued. Therefore, the restart is essential for activation of Endpoint Encryption on the client to proceed.

Endpoint Encryption Status

System restarts as initiated. You will not yet see the PBA page as the Endpoint Encryption software is not yet active on the client. However, you should now be able to see the new option:

- **Quick Settings** | **Show Endpoint Encryption Status** in McAfee Agent System Tray on the client system (EEPC)
- **Encryption** icon | **McAfee Endpoint Encryption System Status** on the menu bar that is present on the desktop of the client (EEMac)

EEAgent synchronization with the McAfee ePO server

The status in the **Show Endpoint Encryption Status** window will show as **Inactive** until EEAgent synchronizes with the McAfee ePO server and gets all the users assigned to it. This is referred to as an ASCI event.

It can be manually triggered on the client by opening the **McAfee Agent Status Monitor** and clicking **Collect and Send Props**. It can also be triggered from the McAfee ePO server by doing an agent wake-up call, otherwise, you will need to wait for the scheduled agent -server communication interval to occur (the default is 60 minutes). After two agent-server communication intervals the status, Endpoint Encryption activation will begin. The activation process requires a number of McAfee ePO events to be sent, and this can take some minutes to occur. Once the client-server communication has completed, the Endpoint Encryption Status will switch to **Active** and encryption will start based on the policy defined.

During EEPC activation, hibernation cannot be used. It is recommended that hibernation is disabled through Active Directory Group Policy while the rollout is in progress. The hibernation feature in EEMac is also disabled when EEMac is active.

User intervention during encryption

The user can continue to work on the client system as normal even during encryption. Once the entire disk is encrypted, the technology will be completely transparent to the end user.

It is safe and risk-free to restart the client system during encryption.

PBA

When the client system is restarted and Endpoint Encryption is first activated, the user should log on with the username that matches the user attribute set in the **EE LDAP Server User/Group Synchronization** task and the default password of **12345** (this is the McAfee default password which can be changed in the User Based Policy) in the PBA page. The user is then prompted to change this password and enroll for self-recovery based on the policy set.

If you want the system to capture the user's credentials automatically without having to make them use a default password on PBA, enable the **Do not prompt for default password** option under **User Based Policies** | **Password**.

We recommend that you change the default password and enforce policies with stronger passwords.

Single Sign On (SSO)

The EEPC client system then boots to Windows. This first boot establishes SSO (if it has been enabled). On future restarts, the user will login to PBA only. Once authenticated, SSO will auto-login to Windows.

In short, the SSO option facilitates the user with the single authentication to the Operating System even when PBA is enabled. Though it requires an extra step, disabling SSO is the more secure configuration.

When the **Must match username** option is enabled, both the EEPC user name and the Windows user name should match for SSO to work, regardless of which domain the user is part of. This user can even be a local user.

When the **Synchronize Endpoint Encryption password with Windows** option is enabled, the EEPC password is reset to the Windows password, however, be aware if the **Password history** option is enabled, and the EEPC password is same as the Windows password, then synchronization will not occur.

On changing the EEPC password, the synchronization will not be reset. Synchronization of the password will occur only when there is a change in the Windows password.

Activate Endpoint Encryption using Add local domain users

Using the **Add local domain users** option, you can activate Endpoint Encryption on the client systems without manually adding users in ePolicy Orchestrator.

The Mac client systems that are added to Active Directory through Directory Utility application are only supported by the ALDU feature. The ALDU feature is not supported on Mac systems that use third party tools like CentrifyDC for Mac, AdmitMac to connect to the Active Directory. EEMac supports ALDU blacklisting using regular expressions.

Task

1. Configure the **Product Settings Policy** with the **Add local domain users** option enabled.
2. Log on to the client system. After the agent to server communication interval, the **Add local domain users** feature adds the previously/currently logged on domain users to the client system.
3. Endpoint Encryption is activated in the client system during the next ASCI. You can now restart the client to log on using the PBA page.

This option provides automatic user assignment, which helps the administrators in not having to manually assign users to client systems in the McAfee ePO console. The recommended best practice is to manually assign at least one user to all systems to ensure that Endpoint Encryption activation happens successfully even if the **Add local domain user** option fails to function as configured. However, if this option is configured correctly, it will not fail. A general recommendation would be to manually add a group of support users to all systems, then activate Endpoint Encryption using the **Add local domain users** option. You can remove these users at a later stage after completing the deployment.

Skip Unused Sectors

Skip Unused Sectors is one of the new features of offline activation that is introduced in EEPC 7.0 Patch 1. For more information about offline activation, see the McAfee Endpoint Encryption - 7.0 Patch 1 Product Guide.

If you have enabled the SkipUnused option, you will have to enter 'Yes' to the message "By using this feature you accept the risk associated with not encrypting unused sectors with respect to (deleted) sensitive data leakage".

5 Operations and maintenance

Managing your systems in different batches, branches or groups will make a great impact for Endpoint Encryption deployment. It is a good practice to arrange the systems in ePolicy Orchestrator in department level or batch level, then deploy the product to these batches one by one.

Managing the servers and client systems

Client deployment in batches with an appreciable number of systems is a good practice by itself.

Please keep the following recommendations in mind while managing the servers and client systems:

- Do not try to create the Endpoint Encryption deployment task at the root level of your system tree and activate it. It is a good practice to deploy Endpoint Encryption to the systems at the sub-level branches.
- Do not deploy EEPC to the server systems, specially the server hosting your McAfee ePO server.
- Secure your McAfee ePO server and database system in the most secured location and keep it accessible for authorized personnel only.

Contents

- *How does disabling/deleting a user in Active Directory affect the Endpoint Encryption user*
- *Manage Machine Keys*
- *Configure role based access control for managing Endpoint Encryption*
- *EEPC 7.0 Patch 1 scalability*

How does disabling/deleting a user in Active Directory affect the Endpoint Encryption user

Every user account has an objectGUID in LDAP. If a user account is deleted from LDAP and another is created with the same user name, this new user account will be a different entity. This is because the objectGUID would have changed for the new user.

To delete a user in LDAP

You must first delete the user in LDAP, then run the **EE LDAP Server User/Group Synchronization** task and send an Agent wake-up call. The user will disappear from EE Users list after the **EE LDAP Server User/Group Synchronization** task is complete.

The ePO Server Settings option **If user is disabled in LDAP server** within **Configuration** | **Server Settings** | **Endpoint Encryption** | **General** | **Edit** can be configured to disable, delete, or ignore the user if the user has been disabled in the LDAP Server. The disable option is enabled by default.

What if a user is disabled from LDAP?

If a user account that is initialized on the client system, and is later removed from LDAP, then it will be automatically deleted/ignored from the client when the next EE LDAP User/Group Synchronization task runs. To authenticate through the client PBA with a disabled or deleted LDAP user name, you should once again enable/add the user to the LDAP and initialize the same user name on the client with the default password.

This does not remove the users from the EEUsers list in ePolicy Orchestrator, however, it removes/deletes/ignores the users from the client system based on the option set in the Server Settings.

Is it possible to just disable the Endpoint Encryption user when removed from LDAP?

It is not possible to disable an Endpoint Encryption user when it has been removed from LDAP. The user is removed from the EE Users list if deleted in LDAP during the next **EE LDAP Server User/Group Synchronization** task.

What if the Endpoint Encryption user assignment is deleted/removed?

If the Endpoint Encryption user assignment is deleted from a system, the user might still be assigned back to the client system if the **Add local domain users** option is enabled in the **Product Settings Policy**. For this to work, the user must have logged on to Windows/Mac at least once and the domain to which client system is connected should have been registered in ePolicy Orchestrator. You can also manually add users using **Menu | Data Protection | Encryption users | Add Users** option in ePolicy Orchestrator.

Manage Machine Keys

The purpose of encrypting the client's data is to control access to the data by controlling access to the encryption keys. It is important that keys are not accessible to users.

The key that encrypts the hard disk sectors needs to be protected. These keys are referred to as Machine Keys. Each system has its own unique Machine Key. The Machine Key is stored in ePolicy Orchestrator database to be used for client recovery when required.

For more information about reusing machine keys, refer to the KnowledgeBase article https://kc.mcafee.com/corporate/index?page=content&id=KB71839.

Machine Key re-use

Machine key re-use option is used to activate the system with the existing key present in the McAfee ePO server. This option is highly useful when a boot disk gets corrupted and the user cannot access the system. The disks other than the boot disks of the corrupted system can be recovered by activating it with the same key from McAfee ePO.

The Machine key re-use feature is not applicable to EEMac, self-encrypting (Opal) drive systems, and UEFI systems.

What happens to Machine Keys when an Endpoint Encryption active system is re-imaged?

All existing data of the system is lost and hence the machine Key is lost when an Endpoint Encryption active system is re-imaged.

What happens to the Machine Key when you delete an Endpoint Encryption active system from ePolicy Orchestrator?

The Machine Key remains in the ePolicy Orchestrator database; however, the key association with the client system is lost when the client system is deleted from ePolicy Orchestrator. When the client system reports back to ePolicy Orchestrator during the next ASCI, it will appear as a new node. A new node does not have any users assigned to the client system. The administrator must therefore assign users to allow login, or enable the **Add local domain user** option in the **Product Setting Policy**. Also, the administrator must configure the required policies in ePolicy Orchestrator.

The next data channel communication after adding the users and configuring the policies will make sure:

- The Machine Key is re-associated with the client system and the recovery key is available.

  When the associated Machine Key is not present with the new node, ePolicy Orchestrator sends a Machine Key request. If the user is logged on to the client system, an agent to server communication between the client and the McAfee ePO server ensures the Machine Key is updated in ePolicy Orchestrator and the users are updated on the client. Thereafter, the Machine Key will be available and admin recovery and policy enforcement will work.

- The users are assigned to the client system. Therefore, these users can straightaway log on to the client system.

What happens to Machine Keys when transferring a client system from one McAfee ePO server to another?

The Machine Key remains in the ePolicy Orchestrator database, however, the key association with the client system is lost when the client system is transferred from another McAfee ePO server.

When a transferred client system reports back to ePolicy Orchestrator during the next ASCI, it will appear as a new node and will therefore not have any users assigned to it. The administrator must therefore assign users to allow logon, assign administrative users to the McAfee ePO branch where the systems are added (by default Lost&Found), or enable the **Add local domain user** option in the **Product Setting Policy**. The administrator must also configure the required policies in ePolicy Orchestrator.

To transfer all systems between McAfee ePO servers, the best process is to follow the ePO Disaster Recovery process. For more information, refer to the KnowledgeBase article https://kc.mcafee.com/corporate/index?page=content&id=KB66616.

The next data channel communication after adding the users and configuring the policies will ensure:

- The Machine Key is re-associated with the client system and the recovery key is available.

  When the associated Machine Key is not present with the new node, ePolicy Orchestrator sends a Machine Key request. If the user is logged on to the client system, an agent to server communication between the client and the McAfee ePO server ensures the Machine Key is updated in ePolicy Orchestrator and the users are updated on the client. Thereafter, the Machine Key will be available and admin recovery and policy enforcement will work.

- The users are assigned to the client system. Therefore, these users can straight away log on to the client system.

What happens to Machine Keys when moving systems from one branch to another in ePolicy Orchestrator?

The LeafNode is not deleted from ePolicy Orchestrator database when a system is moved from one branch to another in ePolicy Orchestrator, hence the Machine Key is available for the particular client system.

How to destroy the recovery information for an Endpoint Encryption installed system?

When you want to secure-erase the drives in your Endpoint Encryption installed system, remove all users from the system (including those inherited from parent branches in the system tree). This will result in making the disks inaccessible through normal authentication as there are no longer any users assigned to the system. You need to then destroy the recovery information for the system using the option **Menu** | **Systems** | **System Tree** | **Systems tab** | **Actions** | **Endpoint Encryption** | **Destroy All Recovery Information** in the ePolicy Orchestrator console. This means that the system can never be recovered.

Configure role based access control for managing Endpoint Encryption

The ePolicy Orchestrator administrator rights management determines what administrators can perform while managing the Endpoint Encryption software.

The administrator can set up Endpoint Encryption specific permission sets to different users in ePolicy Orchestrator. The permission sets can be created for Executive Reviewer, Global Reviewer, Group Admin, and Group Reviewer. The Endpoint Encryption Administrator extension (EEADMIN.ZIP) enables ePolicy Orchestrator administrators to control Endpoint Encryption Systems that are managed through ePolicy Orchestrator.

The McAfee ePO administrator for Endpoint Encryption is able to:

- Manage Endpoint Encryption users, policies and server settings
- Run queries to view the encryption status of the client systems
- View client system audits
- View McAfee user audits
- Manage Endpoint Encryption Providers

Administrative roles can be configured and implemented using the **Endpoint Encryption Permission Sets** option present in ePolicy Orchestrator. It is possible to configure a number of admin roles using this option. For example, you can create admin roles such as:

- **Endpoint Encryption Administrator**: User accounts in this level have full control of Endpoint Encryption, but cannot manage any other software in ePolicy Orchestrator.
- **Endpoint Encryption Helpdesk**: User accounts in this level can do Endpoint Encryption password resets only.
- **Endpoint Encryption Engineer**: User accounts in this level can do password resets as well as export recovery files to be used with EE Tech tool.
- **Endpoint Encryption Auditor**: User accounts in this level can view Endpoint Encryption reports only.

Before you begin

- Make sure that your LDAP server is configured and registered in ePolicy Orchestrator.
- Make sure that you schedule and run the **EE LDAP Server User/Group Synchronization** task.
- Make sure that you enable the **Active Directory User Login** option in ePolicy Orchestrator. To enable, navigate through **Menu** | **Configuration** | **Server Settings** | **Active Directory User Login** | **Edit**, then enable **Allow Active Directory users to login if they have at least one permission set** option.

You can create different permission roles and assign them with different **Endpoint Encryption Permission Sets** to different users.

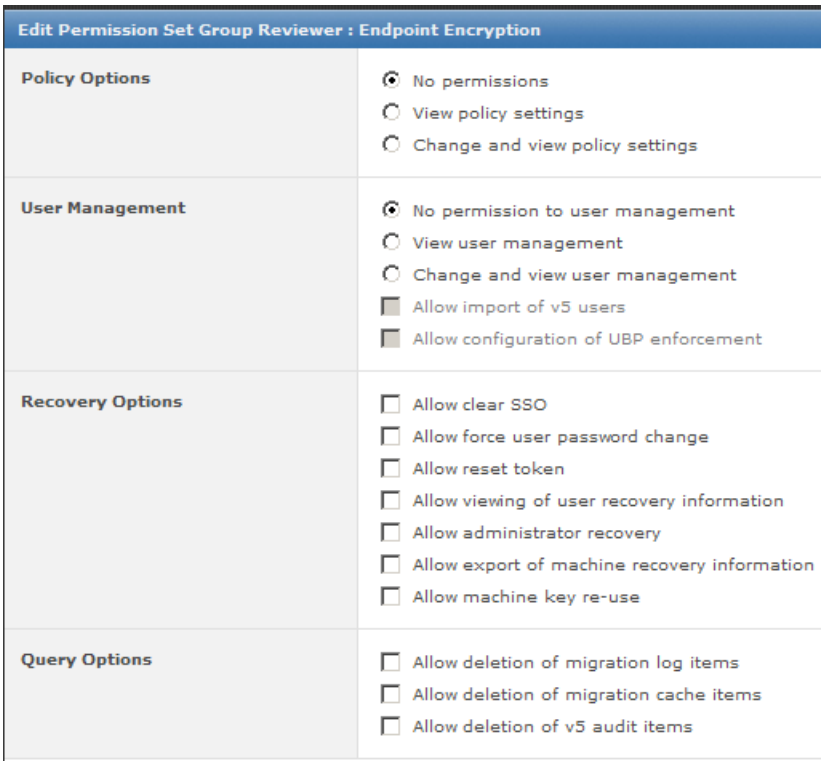


Figure 5-1 Endpoint Encryption permission sets

To verify the configured permission sets, log off from ePolicy Orchestrator, then log on with a user account that belongs to any one of the new roles.

Use correct format of the user name (domain\username) when logging on to ePolicy Orchestrator.

EEPC 7.0 Patch 1 scalability

Use these configurations, recommendations on components, and considerations for scalability.

- ePolicy Orchestrator 4.6 Patch 4
- EEPC 7.0 Patch 1

These considerations and settings will help improve scalability:

- Longer ASCI interval
- Password only deployments should remove certificate query from **EE LDAP User/Group Synchronization** task.

  The User Certificate attribute is used by the McAfee ePO server to determine which certificate should be sent from McAfee ePO to the client, for example, for smartcard tokens. It is better not to query this attribute when you use the Password only token as tests have shown that LDAP query performance decreases when certificates are included in the query. Setting this attribute can also accumulate a large size of data in the database; therefore, you can remove the certificate query from **EE LDAP Server User/Group Synchronization** while using the Password only token.

- Phased rollout during migration, upgrade, or first time installation of EEPC 7.0 Patch 1.

These configurations and factors will degrade scalability:

- **Policy Assignment Rules** — The policy assignment rules should be setup in a logical order to ensure minimal processing. Create an ordered list of rules associated with a User Based Policy. For each user, the rules engine evaluates the rules in order, and the first rule that is satisfied defines which UBP is assigned to the user.

  Make sure that you enable the Policy Assignment Rules for a small number of users to minimize overloading ePolicy Orchestrator.

  Given that ePolicy Orchestrator needs to send all users down to a client during activation, each user will need to have rules run to associate a UBP with them (if UBPs are enabled and rules are defined). With **r** rules, **m** machines and **u** users, the worst case scenario would be an O[n^3] calculation (**r*m*u**), which is not recommended.

  Best practice is therefore to configure the rules in the correct order, such that they are defined in descending order of the number of users that each rule would "catch". For example, if rule A catches 10% of users, rule B catches 80% of users, C 5%, D 2%, E 3%, the most efficient way of ordering the rules would be B->A->C->E->D, if the logic of your rules allows this to be done.

- Large number of user per machine (>20)
- Deployment of unnecessary languages (recovery questions)

The rate of activation can be calculated with the formula, $N_{max}=ASCI_{secs}/M_{upstream}.DC_{rate}$

Where,

- DC_{rate}depends on hardware configuration of ePolicy Orchestrator and Database
- $M_{upstream}$ is the number of data channels (two) being sent from each client

For more details on EEPC 7.0 Patch 1 scalability, refer to the KB article https://kc.mcafee.com/corporate/index?page=content&id=KB71363.

6 Migration and upgrade

EEPC 7.0 Patch 1 has an improved architecture and interface.

Due to these improvements, some functionality from earlier versions of the product is now handled differently.

Contents

- *Best practices for migration and upgrade*
- *Export user assignments from 5.x.x database*
- *Import user assignments to McAfee ePO*
- *Upgrade to EEPC 7.0 Patch 1*

Best practices for migration and upgrade

The information in this section helps you to understand the best practices and prerequisites for EEPC migration and upgrade that involve the following tasks. The detailed procedures to perform the following tasks are given in the *Endpoint Encryption for PC 7.0 Patch 1 Migration Guide*.

- Migrating user assignments from the 5.x.x database to the McAfee ePO server
- Exporting from 5.x.x database
- Importing the export file (the user information) into the McAfee ePO server that has EEPC 7.0 Patch 1
- Exporting audit information
- Importing audit information
- Upgrading the client system from EEPC 5.x.x
- Upgrading the client system from EEPC 6.x

Migration tool

Make sure that you have the latest **EEMigration.ZIP** file of EEPC 7.0 Patch 1 to implement and perform the export. We recommend that you copy and extract the **EEMigration.ZIP** file to the folder where **Endpoint Encryption Manager** (EEM) is installed.

Exporting 5.x.x database

- Make sure that you have access rights to view system and user properties on Endpoint Encryption Manager and the McAfee ePO server.

Importing the systems or users from 5.x.x database into the McAfee ePO server

- Make sure that 5.x.x and 7.0 Patch 1 are connected to the same LDAP server during the export and import process.
- Make sure that you have registered an LDAP server on the McAfee ePO server before initiating the import process.
- Make sure that you have scheduled and run the **EE LDAP Server User/Group Synchronization Server** task before initiating the import process.
- Analyze the color-coordinated results in different phases of the import. It guides you to make appropriate decisions before proceeding to the next step.
- Do not navigate away or shut the browser when the import is running on ePolicy Orchestrator. Doing so interrupts the import thread and stops the import process. When the import is running, you can see the message **Please wait, assigning users to systems** in the top left of the McAfee ePO console.
- After you import the systems or users from 5.x.x database into the McAfee ePO server, check that the systems, users, and the audit details are imported as you expected. Check that the password token, self recovery, SSO details, if available, are imported as you expected.
- Conduct a policy review after the import process. If you need your 5.x.x policy settings for 7.0 Patch 1, you must set them before upgrading the client. Make sure that you enable the Encrypt product setting policy under **Endpoint Encryption 7.0.1 | Product Settings | Encrypt**. If this is not set, encrypted client system starts decrypting by default.

  To initiate the encryption on the client, you must select any one of the options other than **None**. The default option **None** does not initiate the encryption.

  Some firewall software enforce HTTP session timeouts. During the import you should review your firewall settings according to the manufacturer documentation and take the necessary actions to prevent the firewall from timing out the session.

- Before upgrading the client, make sure that the user's UBP enforcement settings are correct and the appropriate Policy Assignment Rule is created on McAfee ePO if those users are intended to use the non-default UBP.

Upgrading to Endpoint Encryption 7.0 Patch 1

- Make sure that the system to be migrated is managed by the McAfee ePO server.
- Migration of users directly from 5.x.x client to the new EEPC 7.0 Patch 1 client is not supported. Any migration of user assignments must be done on ePolicy Orchestrator before or after deploying EEPC 7.0 Patch 1 to the client system.
- To upgrade the client, first install the EEAgent, then the Endpoint Encryption software packages.
- If 5.x.x users are found in the assigned LDAP OU/Group, the 5.x.x password token, SSO and Self Recovery data will be transferred to EEPC 7.0 Patch 1. If new users are present in the assigned LDAP OU/Group, then they are added to EEPC 7.0 Patch 1, as users not being initialized.
- When upgrading from EEMac 1.x/6.x to EEMac 7.0 Patch 1, make sure that you restart the client system when prompted. EEMac services will not be available until you restart the client system.

General recommendations

- Retain the 5.x.x database for some time, so that you can access it case any loss or theft of a device after the migration.
- Migrate only a small number of systems as an initial test before doing a large-scale migration.
- If you are using the $autoboot$ user id in 5.x.x to boot your systems without actually having to authenticate through the PBA, then please be advised that the same option is now a feature in 7.0 Patch 1. So, make sure that you enable this option (**Menu | Policy | Policy Catalog | Endpoint Encryption 7.0.1 | Product Settings | Logon | Enable Automatic Booting**) to activate **Autoboot** while migrating the users and systems from 5.x.x to 7.x. To enable automatic booting without adding a user, you need to configure the **Add local domain users** feature.

The Enable Automatic Booting option in the Product Setting Policy allows access to the EEPC installed systems without actually having to authenticate through PBA. However, it is the administrators' responsibility to ensure that system security is not compromised if this option is selected.

If you enable this option, be aware that the McAfee Endpoint Encryption software doesn't protect the data on the drive when it is not in use.

Export user assignments from 5.x.x database

The export tool provided with EEPC allows the administrator to export the user assignments from 5.x.x database. The purpose of exporting the user assignments is to reduce the amount of configuration required by the administrator to upgrade from 5.x.x to 7.x.

The export output is a .ZIP file, which can be imported into the McAfee ePO server. The import process uses an import wizard on the McAfee ePO server after installing the applicable EE extensions.

The purpose of exporting systems from 5.x.x database is to export the user assignments. Migration export is not required if you do not want to migrate the user assignments.

Best practices

- Make sure that you have the latest **EEMigration.ZIP** file from the EEPC 7.0 Patch 1 release package to implement and perform the export from 5.x.x Endpoint Encryption Manager.
- We recommend that you copy and extract the **EEMigration.ZIP** file to the folder where Endpoint Encryption Manager is installed.
- Make sure that you have the access rights to view system and user properties on EEM and the McAfee ePO Server.

- It is important to understand the export options; **Machines** and **Users** in the export wizard. You can select any one of the options to export the required user assignments from 5.x.x Endpoint Encryption Manager.
  - On selecting the **Machines** option in the export wizard, all users assigned to the selected machines from 5.x.x database are exported. This also provides the option to select specific machine, so that all the user assigned to that particular system can be exported.
  - On selecting the **Users** option in the export wizard, all systems to which the selected users are assigned are exported. This also provides the option to select specific users so that all the systems that have the selected users are exported.
- By default, system or user audit event data is not exported. It is the responsibility of the administrator to select the **Export Machine and User audit events** option during the export process.

Importing the audit logs increases the size of the McAfee ePO database. We recommend that you keep the number of days as minimum as possible.

Import user assignments to McAfee ePO

The Endpoint Encryption Admin extension provides a user interface to import the export file (.ZIP) created during the export from 5.x.x administrator system.

Important prerequisites for importing user assignments

- Make sure that you have the permission to **Allow Import of v5 users** to perform this task. You can enable this permission by navigating through **Menu | Users | Permission sets | Endpoint Encryption | Allow Import of v5 users**.
- Make sure that you have copied the export file (.ZIP) to a location where you can access it from the McAfee ePO server.
- Make sure that the systems to be upgraded are managed by ePolicy Orchestrator.
- Make sure to register the LDAP server on the McAfee ePO server and make sure it is the same server registered on the 5.x.x database.
- Schedule and run the server task **EE LDAP Server User/Group Synchronization** before initiating the import process.

Key notes on importing user assignments

- If users were manually added to the 5.x.x database and the same users were not present in the Active Directory, then that 5.x.x users will appear as unmatched users in ePolicy Orchestrator during the import process. In this situation, you need to make sure that you assign these unmatched users to configured LDAP users.
- EEPC 5.x.x users disabled in the Active Directory will be imported to ePolicy Orchestrator during the import process, however, the properties of these disabled users will be determined by the Endpoint Encryption Server Setting configured in ePolicy Orchestrator.
- The application performs the system matching using the 5.x.x machine name and the McAfee ePO system name. The results are color-coordinated, so that it is easy for the administrator to analyze the results.
  - Green indicates a successful matching
  - Red indicates an unsuccessful matching
- The application performs the user matching using the binding attributes if they are present. If no match is found, the rules are used to search every LDAP server that has been set up with EE LDAP

attributes. The results are color-coordinated, so that it is easy for the administrator to analyze the results.

- Green indicates a single match
- Orange indicates more than one match
- Red indicates no match

Do 5.x.x policies get imported to 7.x during the migration?

No, 5.x.x policies are not imported to 7.x as part of the migration process. The user should set the required 5.x.x policies, more importantly the **Encrypt** policy, in 7.x before upgrading the client.

If you do not change the default **Encrypt** policy from **None** to **Encrypt** in 7.x before the upgrade, the client system will start decrypting after the upgrade. So, it is always a best practice to configure your required policies before even initiating the import process.

What happens if the LDAP server used by 5.x.x is not registered in ePolicy Orchestrator?

All imported users of 5.x.x will appear as unmatched users in ePolicy Orchestrator. So, ensure to register the same LDAP server used by 5.x.x, then schedule and run the **EE LDAP Server User/Group Synchronization** task.

What happens if the LDAP server has been registered, but the EE LDAP Server User/Group Synchronization task hasn't been scheduled and run?

ePolicy Orchestrator will display an error message when the user initiates the import process. Closing the error message will guide the user directly to **EE LDAP Server User/Group Synchronization** task page.

What happens if the 5.x.x machines are not managed by ePolicy Orchestrator?

All imported machines of 5.x.x will appear as unmatched machines in ePolicy Orchestrator. So, make sure that the systems to be migrated are managed by ePolicy Orchestrator before initiating the import process.

Upgrade to EEPC 7.0 Patch 1

The primary goal of upgrading the EEPC 5.x.x series to EEPC 7.x is to retain the disk encryption. This is to make sure that a decrypt and a re-encrypt of the disk is not required during the upgrade.

Only one encryption algorithm can be active for all disks, so no matter whatever the algorithm is set in 7.x, if the 5.x.x system has a different algorithm, then that algorithm will be used for all disks even after migrating to 7.x.

The only way to change the client algorithm is to deactivate EEPC on the client and decrypt all disks, then reactivate EEPC on it.

All the recovery settings have 4 times as many lines as the AES algorithm. So, setting recovery key size as **Low** gives 4 lines of response code with RC5 algorithm.

On migrating from EEPC 5.x.x to EEPC 7.x, the available user password token, SSO, and Self Recovery details are transferred to EEPC 7.x. To use 5.x.x SSO and Self Recovery data in 7.x, you need to enable Self-Recovery and SSO in the 7.x policies after importing the users.

What happens to a partially encrypted 5.x.x system after the migration?

A partially encrypted 5.x.x system gets fully encrypted or decrypted as per the policies set in 7.x.

What happens if the user initiates the upgrade process while the 5.x.x client is still in encrypting or decrypting state?

It completes the encryption or decryption process as per the policies set in 7.x.

What happens to a removable media that is encrypted with 5.x.x?

We recommend that you decrypt your removable media before initiating the upgrade.

Be aware that there is no way to decrypt your removable media after the upgrade, other than using the EETech recovery tool.

Are the 5.x.x token details migrated to 7.x?

Yes, 5.x.x Password token details are migrated if it is available.

Are the SSO and Self Recovery details migrated from 5.x.x to 7.x?

Yes, the SSO and Self Recovery details are migrated from 5.x.x to 7.x only when the 5.x.x Password token is available. The user needs to enable SSO in the 7.x Product Settings Policy and Self-recovery in corresponding User Based Policy. The user does not have to enroll again for Self Recovery when the product is upgraded from 5.x.x to 7.x.

What happens to a 5.x.x system after migration if it has been encrypted using an algorithm that is different from 7.x?

The system remains encrypted with same algorithm as set in 5.x.x, and you can apply all the policies of 7.x to the migrated system as usual. To change the algorithm, you need to first deactivate EEPC, change the algorithm, then activate.

7 Use ePolicy Orchestrator to report client status

McAfee ePolicy Orchestrator provides comprehensive management and reporting tools for Endpoint Encryption.

Administrators can create standard and customized dashboards, queries, and reports. The procedures on how to create standard dashboards, queries, and reports are documented in the *McAfee Endpoint Encryption - 7.0 Patch 1 Product Guide*.

When the EEAgent software package is deployed to the client systems and they are successfully managed by ePolicy Orchestrator, then any of the following queries can be used to retrieve data:

- EE: Disk Status
- EE: Encryption Provider
- EE: Installed Version
- EE: Users
- EE: Product Client Events
- EE: Disk status (Rollup)
- EE: Installed version (Rollup)
- EE: Migration log
- EE: Migration lookup
- EE: Volume status
- EE: Volume status (Rollup)
- EE: V5 audit
- Intel® AMT out-of-band queries

Contents

- *Track the progress of the deployment and encryption status*
- *Report encryption status from McAfee ePO*

Track the progress of the deployment and encryption status

The progress of the EEPC/EEMac deployment and the number of encrypted drives can be easily determined by running the Endpoint Encryption query under **Menu** | **Reporting** | **Queries** | **Endpoint Encryption** | **EE: Disk Status**. This will report the crypt state for all disks on systems that have the EEAgent installed.

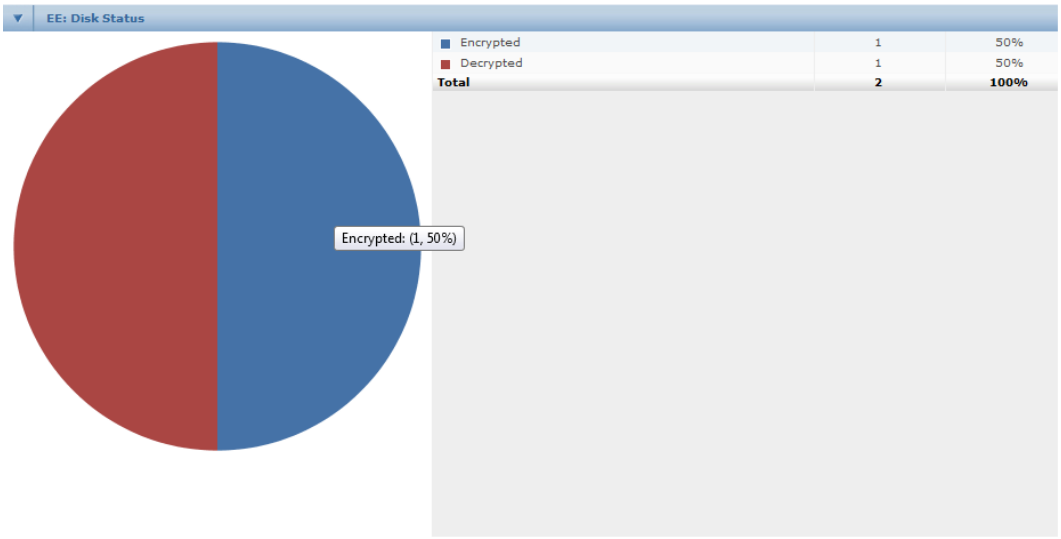


Figure 7-1 Endpoint Encryption disk status

You can also find the systems that don't have the EEAgent installed by running the query **Menu** | **Reporting** | **Queries** | **Endpoint Encryption** | **EE: Encryption Provider**.

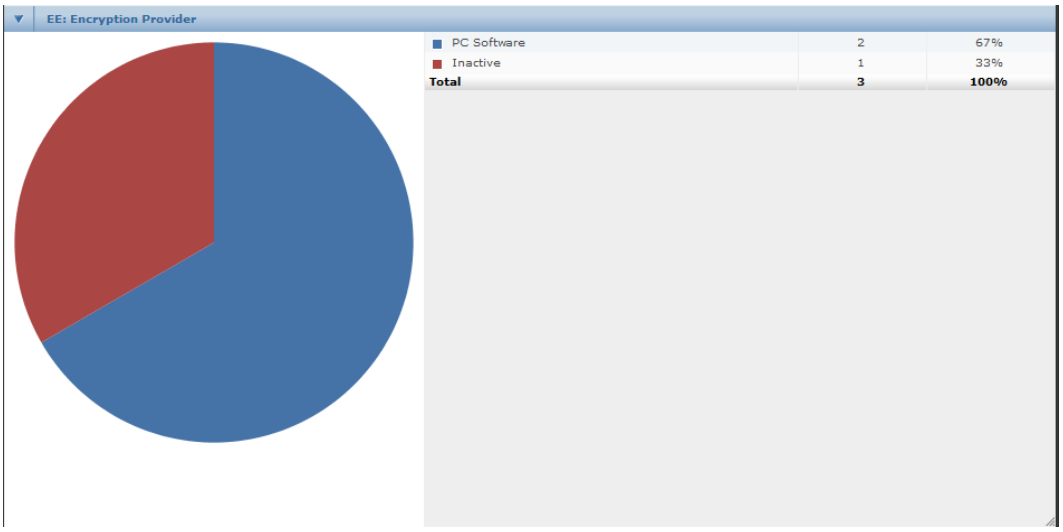


Figure 7-2 EE: Encryption provider

Report encryption status from McAfee ePO

To comply with data protection regulations, IT staff must be able to produce evidence that a suitable technical measure was in place to protect sensitive information on, for example, a missing computer.

The organization must encrypt the device and be able to prove that the device is encrypted after it is reported lost or stolen.

High level process

Endpoint Encryption makes this task easy. An administrator can log on to McAfee ePO and, in just a few clicks, be able to produce a report showing that the missing computer was encrypted.

- Log on to ePolicy Orchestrator as an administrator.
- Locate the system in the System Tree.
- In the McAfee ePO server, drill-down to encryption properties.
- Check the encryption status under the Disks tab.

Finding the user's system in ePolicy Orchestrator

The encryption status is stored as a property of the system, not the user. To confirm that a missing computer is encrypted, you must find the system in ePolicy Orchestrator and view its properties. You can use the queries and reports to know the encryption status of the system.

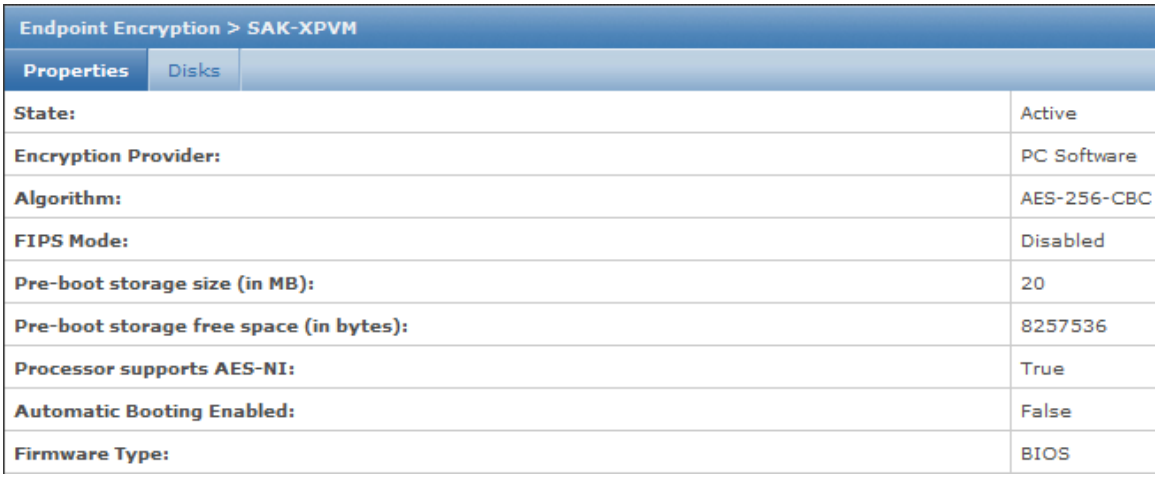


Figure 7-3 Endpoint Encryption system properties

Index

A

abbreviations 8
about this guide 5
activation 33
AD 16, 36
add local domain users 20, 39, 42, 45, 46
add users 16
Agent wake-up call 41
algorithm 55
AMT, out-of-band actions 30
ASCI 9, 10, 42, 46, 49
audit events 53
authentication 12
auto boot 33, 39, 42
    configure 31

B

backup 34
best practices 7
BIOS 11, 12
boot sequence 12

C

client events 57
client status 57
client system 36, 45
conventions and icons used in this guide 5

D

data protection 11
default password 39
deployment 33, 36
deployment progress 58
design overview 9
disable user 45
disk check 34
disk status 57
display name 17
documentation
    audience for this guide 5
    product-specific, finding 6
    typographical conventions and icons 5

E

EEAdmin 36
EEAgent 10, 20, 36, 39, 41
EEGO 13
EEM 51, 53
EEMac 7
EEPC 7, 11, 12, 20, 31, 33, 36, 39, 41, 45, 46, 48, 49, 51, 58
EEPC extension 36
EEPC package 36
EEPC/EEMac 16, 57
EETech 33, 34
Enable Automatic Booting 20
encrypted 55
encryption 7, 20, 31
encryption provider 20, 57, 58
encryption status 41
Endpoint Encryption 12, 39
export 53

G

group users 39

H

HDD 9

I

import 36, 54
IP Address 16

L

LDAP 16
LDAP server 15, 17, 36, 39, 45, 48, 49, 54
LDAP synchronization 17
Log on 20

M

machine keys 46
machines 53
maintenance 45
MBR 12
McAfee Agent 12
McAfee ePO 12, 15, 16, 39, 41, 45, 46, 51, 53, 58

McAfee ServicePortal, accessing 6
migration 51

O

Opal 9, 46
operations 45
OU 16, 39

P

password 28, 39
PBA 7, 11, 20, 33, 39, 41, 42, 45, 51
permission sets 48, 54
phased deployment 15, 31
pilot test 34
policies 7
    Product Settings Policy 10
    User-Based Policy 10
pre-boot smart check, enabling 20
preparations 34
Product Settings Policy 20, 36, 39, 42, 45, 46
purpose 7

Q

queries 31, 58

R

readers 34
recommendations 34
recovery 34
recursive 16
remediation
    out-of-band 30
report 31, 57, 58
reporting encryption status 58
requirements 12
requirements testing, EEGO 13
requirements testing, pre-boot smart check 13
Role Based Access Control (RBAC) 48

S

samaccountname 17
scalability 49
self recovery 28, 39, 55
server 45, 51
server name 16
server settings 45
server task log 17
ServicePortal, finding product documentation 6
SSO 20, 41, 51
System Tree 36

T

TCG 9
Technical Support, finding product information 6
token 34, 51, 55
token type 10, 28

U

UBP enforcement
    configure 10
    disable 10
    enable 10
unlock PBA
    out-of-band 30
upgrade 51, 55
user 34, 39, 48, 53
user assignments 53
user certificate 17
user management
    out-of-band 30
User-Based Policy 28, 39
username 17
users 54